CULTURE DIMENSIONS OF INFORMATION SYSTEMS SECURITY IN SAUDI ARABIA NATIONAL HEALTH SERVICES

Saleh Al-umaran

A thesis submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy

Software Technology Research Laboratory

(Faculty of Technology)

De Montfort University

February 2015

Abstract

Organisation information security culture has become one of the most important elements of an organisation's strategy, to promote its image, performance and efficiency. The study of organisations' information security cultures has interested scholars, as well as the healthcare service industry, to research the topic and find appropriate tools and approaches for developing a positive culture. Health service information increased sharply in recent years due to the increase in expanding healthcare services as well as the use of electronic recording processes. Healthcare providers need to ensure the security of the information that they receive due to an increase in numbers of patients who are wary about providing personal medical details and complying with national and international legislation. This is to avoid any disputes with providers and stakeholders. The vast majority of studies on the Saudi National Health Service are on the use of technology to protect and secure health services information. On the other hand, there is a lack of research on the role and impact of an organisation's cultural dimensions on information security. Several researchers in the literature argue that information security needs to be focused on the organisation's behaviour, (McIlwraith, 2006; Da Veiga, A., and Eloff, J., 2010; Van Niekerk and Von Solms, 2005). They stressed that the organisation's success or failure depends largely on the employees' behaviour towards information security. They indicated that an information security-aware culture would minimise risks to information assets and specifically reduce instances of employee misbehaviour. This research aims to investigate and analyse the role and impact of cultural dimensions on information security in Saudi Arabia's health service. Two surveys

have been carried out in order to collect data and information from three major hospitals in Saudi Arabia. The first survey aimed to identify the main cultural dimension problems in the Saudi Arabian health service and develop an initial information security framework model. The second survey evaluated and tested the developed framework model for its usefulness, reliability and applicability. The developed model contributed to promoting a strong information security culture and developing appropriate information security culture policy and guidelines.

Acknowledgements

I would like first to express my deepest appreciation and lasting gratitude to my first supervisor, Dr Giampalo. His wide knowledge and logical ways of thinking have been of great value to me. His understanding, encouragement and personal guidance have provided a good basis for the present thesis. Without his guidance, the successful completion of the research and this thesis might have been a very difficult task. His critique and helpful ideas have shown me the way to proceed. I am truly grateful for that. I genuinely appreciate his positive comments, which have improved and brought out the optimum consequences from my endeavours.

I would also like to express my gratitude to the Professor Hussein Zedan, the former director of Software Technology Research Laboratory (STRL), and Dr F. Chen for their unlimited support and advice throughout this work. I appreciate their positive comments, as they have brought about optimum consequences from my endeavours.

I wish also to express my sincere thanks and appreciation to my father and mother for their continuous encouragement and emotional support all the way through my studies, and my brothers and sisters who with their support have inspired me to achieve my goal.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

EPR	Electronic Patient Record
KFH	King Faisal Hospital in Riyadh
ICT	Information and Communication Technology
IS	Information Security
ISM	Information System Management
MIS	Management Information System
NHS	National Health Services
SA	Saudi Arabia
SA NHS	Saudi Arabia National Health Services
SPSS	Statistical Package for Social Sciences
UN	United Nations

CHAPTER 1
INTRODUCTION

Chapter 1 Objectives

The main objectives of this chapter are as follows:

- To provide justification for the research;
- To clarify and state the primary research aims and objectives;
- Providing background of the Saudi Arabian health services;
- Highlighting the researches main contributions;
- To provide the thesis structure.

Chapter 1 Introduction

1.1 Introduction

On a global scale, information has seen sharp changes in the last few decades in their operations and the rights of patients and staff members' to their personal information. It has also shifted from traditional handling and accessing of patients and staff information to the effective use of electronic technology. This has led to understanding the importance of, and needs for, effective policy and strategy to ensure the security of health services information. Effective information security also helps in improving and promoting health services (Marchibroda, 2007).

Cultural dimensions have become an important part of an organisation's strategy to promote its performance and productivity. The study of organisations attracted scholars as well as the health service industry to research the topic and find appropriate tools and approaches to develop a positive culture. There are a large number of studies on the role of culture dimensions on society and organisations. One of the main contributions in this area is Hofstede's work (1980, 1997, 2001). Eloff et al. (2003) argued that organisations need to change to the holistic management of information security to establish an effective information security culture. The vast majority of studies regarding Saudi National Health Service are on the use of technology to protect and secure health services information. On the other hand, there is a lack of research on the role and impact of organisations' cultural dimensions on information security. Da Veiga et al. (2010) argued that information security needs to be focused on the organisation's behaviour. They stressed that the organisation's success or failure depends on the employees' behaviour within the organisation. They indicated that an information security-aware culture would minimise risks to information assets and specifically reduce rates of employee misbehaviour.

Saudi Arabia is in the process of developing its institutions and healthcare system to cope with the socioeconomic changes of the Kingdom, as well as regional and internal changes. The main challenges in the Kingdom's development processes are in using technology in management.

One of the main challenges of the introduction and implementation of technology is the cultural changes that will occur as a result. Cultural change can be found at the organisational and national levels.

The Kingdom has no problem investing in technology, hardware and software due to the large revenue that it receives from oil. The challenge of the Kingdom is in investing such revenue in developing its institutions such as the healthcare services.

Information can be protected by two strategies. The first is the use of technology to protect valuable information, which is required when intruders try to access and transfer information. The second is the human element, wherein the user can either deliberately or accidentally abuse the information by passing information to a third party without consent of the information owners. This research is focusing on the role of the human element of the health services culture on information security. The main reasons for focusing on human include large number of research carried out in use of technology, lack of research in role of human, and the human factor is challenging to monitor and control.

1.2 Research Aims and Objectives

This section presents the following main research aims and objectives.

1.2.1 Research Aims

This research aims to investigate and analyse the role and impact of cultural dimensions on information management systems security in the Saudi Arabian health service.

1.2.2 Research Objectives

The main objectives of the research that lead to the fulfilment of the research aim can be summarised as the following:

- To carry out a critical analysis of the related literature on information security culture in healthcare service providers;
- To identify and analyse information security culture dimensions;
- To collect quantitative and qualitative data evaluating the designed information security culture model;
- To develop and design the information security culture model for SA health services;
- To evaluate the designed information security model;
- To provide recommendations to improve, enhance and promote the information security culture in SA health service.

1.3 Research Background

Saudi Arabian health services have seen rapid growth in recent years to cope with the estimated population of 26 million with an annual growth rate of 2.2% (Walston et al., 2008; Almalki, 2011). The growth in health services is needed to cope with population growth as well as citizens' understanding and awareness of their right to receive the appropriate healthcare services.

Almost 60% of hospitals in Saudi Arabia are managed, owned and controlled by the Saudi government, namely by the Ministry of Health. The hospitals' main objectives include providing basic health care services to nationals and non-nationals. Saudi Arabia has a large number of non-national workers in its various industries. It is important to stress that Saudi Arabia has introduced and implemented mandatory health coverage for all expatriates working in Saudi Arabia, and they are in the process of implementing this coverage to Saudi nationals. The Saudi authority established the Council for Cooperative Health Insurance in 1999. The main role of the council is to introduce, regulate and supervise the implementation of appropriate health insurance strategies for the Saudi health care market (Walston et al. 2008). The main effect of such implementation is the pressure on health care providers to avoid any legal, (Gerber and Solms, 2008), disputes with insurance companies, such as the handling of patients' medical records (Kingdom of Saudi Arabia Healthcare Overview, 2012).

Decentralisation and the Private Sector

The Ministry of Health is under pressure from authorities and pressure groups, such as the media, to cope with high health service operations demands, sharp increases in budget requirements, and meeting the needs of patients and their families. These pressures have led

the Ministry of Health to give the regional directorates some authority in terms of planning, recruitment of healthcare staff and contracting health care providers within a certain budget. The second strategy is intended to reduce pressure on the Saudi Arabia Ministry of Health and to improve the quality of the health services used to support and encourage the private health sector. It argues that the privatisation of some of the healthcare services in SA helps in speeding up the decision-making process, reduces care costs, produces new income resources for health care and creates competition in the health market. This can lead to improvement in the quality of health care.

It is also important to stress that the SA health authority is adopting e-health initiatives to improve the services that it provides (Househ et al., 2010). One of the main challenges faced by the health service is the security of electronic patient records and the necessity to save 10-15% of the public health budget (Aldajani, 2011).

One of the main problems in the SA health care services is the lack of clear and effective regulation to protect electronic patient records and the implementation of appropriate protection policies (Aldajani, 2011). This leads to the importance and necessity of research, providing academic evidence to enhance and promote health information security. This research's main aims are to explore and identify health information security culture and to provide appropriate framework to enhance information security.

1.4 Research Questions

The researches main outcomes need to provide an appropriate answer to the research question, (Clough et al., 2002). This study's main findings aim to provide answers and clear explanations to the following research questions:

What is the role of cultural dimensions on information security in the SA National Health Service?

The above research question can be answered by answering the following sub-questions;

Q1: What is the current situation of information security culture in the SA National Health Service?

Q2: What are the main cultural dimensions and sub-dimensions influencing the information security culture of the Saudi National Health Service?

Q3: What is the structure of the information security culture framework model?

Q4 How reliable, practical and useful is the framework to Saudi Arabia's National Health Service?

1.5 Research Hypotheses

The research main hypothesises are as follows:

Hypothesis 1:

H1: Organisational leadership is positively related to the employees' attitude towards health information security.

Hypothesis 2:

H2: Employees' job satisfaction and job security are positively related to the employees' attitude towards information security.

Hypothesis 3:

H3: Trust is positively related to the employees' attitude towards information security.

Hypothesis 4:

H4: Saudi national culture is positively related to the employees' attitude towards information security.

Hypothesis 5:

H5: Organisations' communication is positively related to the employees' attitude towards information security.

Hypothesis 6:

H6: Employees' intentions towards information security are positively related to the employees' attitude toward information security.

Hypothesis 7:

H7: Hospital multicultural backgrounds are positively related to information security.

1.6 Importance of the Research

Health services in Saudi Arabia have expanded in the last few decades, and the implementation of information security systems has become an essential part of health services. There is an extensive amount of research that focuses on the technical elements of information security in health services with a clear lack of research on the role and impact of the hospital culture on information security. Therefore, it is one of the challenges of the SA health service to establish and promote an appropriate and positive information security culture among the health service providers in the Kingdom. The health services lack any framework for the information security culture that the healthcare authority can use and adopt. This study is the first research in the field measuring the role and impact of culture on information management in Saudi Arabia. The framework can be used as part of the authority's strategic planning on information security policies, employees' training and the structure and activities of health services. It is also important to stress that SA patients have become more aware of their rights to their personal information and the importance of maintaining security and safety in the handling of their information. The patient's rights may include the rights to undertake legal disputes with health service providers in the event that their information has been handled wrongly or misused.

1.7 Research Plan

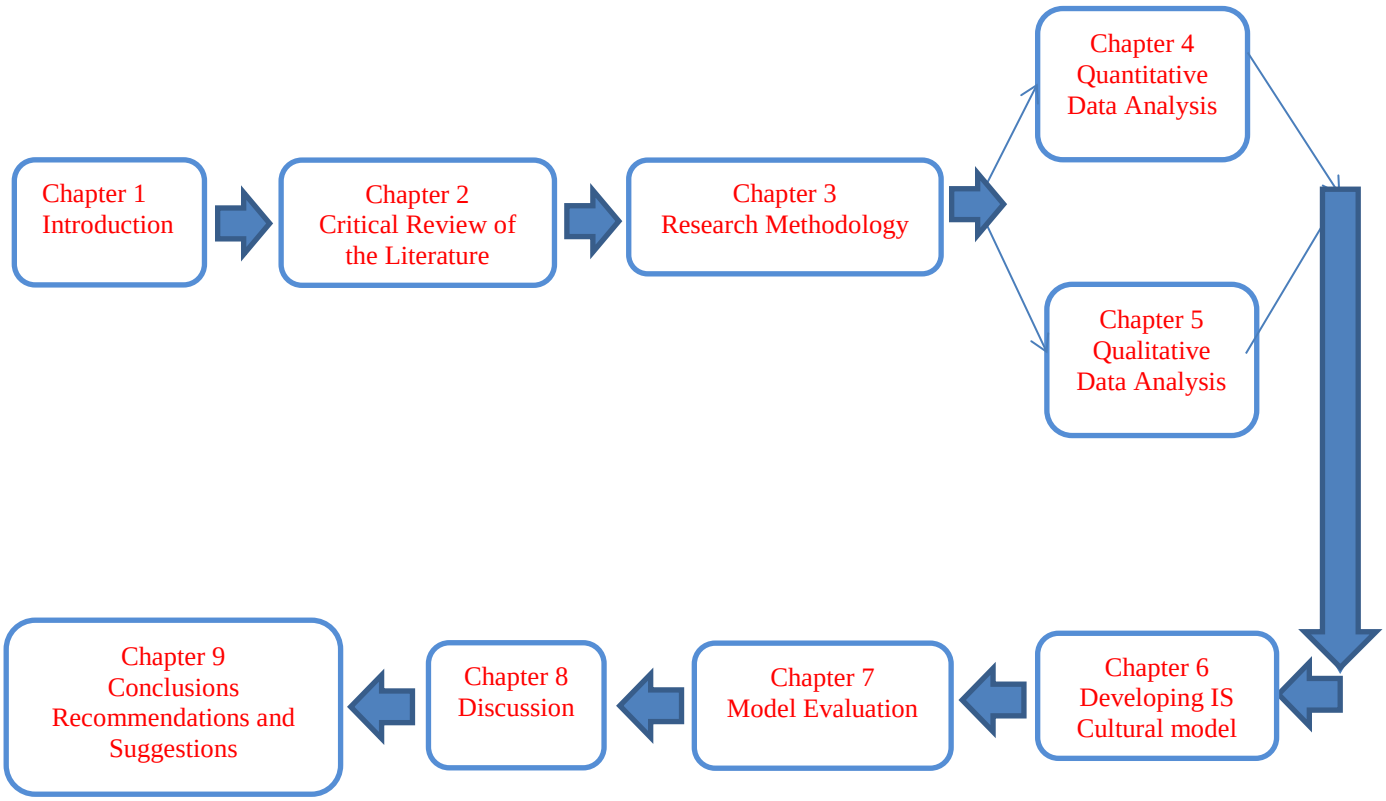

Figure 1-1: Research plan process

1.8 Thesis Structure

The thesis is organised into the following chapters.

Chapter 1: Introduction

This chapter presents the research's main aims and objectives and provides justifications for carrying out the research. The chapter also provides a brief background of the Saudi Arabian Health Service.

Chapter 2: Literature Review

This chapter critically reviews related literature in order to establish the research framework. The chapter focuses on the information security culture and its role on implementing and developing information security culture policies.

Chapter 3: Research Methodology

This chapter presents the main research methodology adopted to achieve the research aims and objectives. The chapter also provides justifications for adopting the tools and processes used to collect the quantitative and qualitative data and the selected samples, as well as the pilot study used.

Chapter 4: Data Analysis: Quantitative Data Analysis

This chapter presents a data analysis of the first fieldwork visit. This data analysis is intended to identify the main information security culture dimensions that influence the information security culture of the SA health service.

Chapter 5: Data Analysis: Qualitative Data Analysis

This chapter presents analyses of one-to-one, in-depth interviews conducted with key health service employees. The chapter aims to explore the information security culture and provides evidence to support the main outcomes of the quantitative data analysis of Chapter 4.

Chapter 6: Information Security Culture Modelling

This chapter presents and discusses the developed information security culture model based on the main outcomes of the data analysis, located in Chapters 4 and 5, and the literature review in Chapter 2.

Chapter 7: Model Evaluation: Quantitative and Qualitative Data Analysis

This chapter presents a critical evaluation of the developed information security model. The evaluation aims to explore the SA health service officials' opinions and attitudes towards the developed information security culture dimensions and the relationship between dimensions.

Chapter 8: Discussions

This chapter presents discussions and a critical evaluation of the research's main outcomes and provides answers to the research questions and hypotheses.

Chapter 9: Conclusions, Recommendations and Suggestions for Future Research

This chapter summarises the research's main outcomes and the main contributions of the research. The chapter also provides recommendations to improve the information security culture within Saudi Arabia's health services fields. The chapter closes with suggestions for future research in the area of information security culture in SA.

CHAPTER 2
LITERATURE REVIEW

Chapter 2 Objectives

The main objectives of this chapter are as follows:

- To clarify and define related terms to information security;
- Critically reviewing related literature on information security;
- Identifying information security culture dimensions.

Chapter 2 **Literature Review**

2.1 Introduction

Organisation culture has become an important part of an organisation's strategy to promote its performance and productivity. The study of organisation culture's role on information security has attracted scholars as well as industry leaders to research the topic and find appropriate tools and approaches to develop positive information about security culture.

In any society or organisation, individuals need to be able to interact with each other based on a set of accepted rules and values. These rules and values need to be complied with and accepted by society and organisations. These rules are usually developed over a long period of time and rooted with their personal characteristics and values. These rules encompass certain values and traditions that will be part of an individual's daily activities. It is also important to stress that these values and norms will become an identity for the society or the organisation. The society or organisation will be known and identified by these values and norms such as the generosity of the Bedouin in Arab society.

Information security has become one of the main concerns of organisation management and has become one of the information management strategies. Health care service providers manage, control and transmit large amounts of information in traditional, hard copy and electronic records. The health service information security has become one of the main challenges that health service authority's worldwide face.

This literature review aims to explore and provide an understanding of the influence of organisation culture and national culture on information security with a specific focus on the role and impact of the health service culture on information security. The literature review also aims to help in developing the research framework.

The literature review starts with definitions and discussions of the terms and related issues of information security, privacy and confidentiality. This will be followed by a discussion of culture in general terms and its role on an organisations performance. The literature closes with a discussion of the role of the health service culture on information security. The chapter closes with a summary of the main findings of the reviewed literature.

2.2 Information Security

The core of this research is information security in health care services in Saudi Arabia. Therefore, it is important to explore the term information security in-depth in order to understand and be aware of its meaning. The term security can denote that there are enemies, whilst *safety* refers to the necessity of dealing with such risks in normal circumstances (Pieters, 2011). At first sight, information security can be regarded as the distinction between what needs to be protected and its environment and the main task, which is determining how to protect the information from its external environment. Information must be managed and controlled in a certain environment. Information needs to be protected in appropriate and accounted measures.

From the organisation's point of view, information security has become one of the challenges for their operations and management (Rotvold, 2008). Reed (2007) argued that information security is reaching a crisis point and that it is one of the main problems facing companies. The author

stressed that this is mainly due to the impact of breaching information security on a large number of the organisation's stakeholders.

One of the main aims of information security is to provide appropriate and effective tools and mechanisms to protect the integrity, confidentiality and availability of information from any unauthorized access as well as attacks on such information (Pieters, 2011; Kruger & Kearney, 2006). The authors argued that confidentiality referred to protecting against any unauthorised reading of information. This includes accessing a patient's electronic records.. Integrity of information refers to any unauthorised writing. This includes any editing of existing records, such as updating and adding information to a patient's record without authorisation. Finally, availability refers to any unauthorised deletion of information (Pieters, 2011). This includes the fact that unauthorised individuals are not permitted to delete any patient's electronic records, nor are they permitted to destroy hard copies of a patient's traditional medical record.

2.3 Information Privacy

Individual privacy has become increasing important in modern society due to awareness and legislation to protect people's privacy (Deng et al., 2011). It has become extremely critical that both traditional and digital information needs to be protected to prevent any intruders from unauthorised access and use of such information. Therefore, it is not surprising to stress privacy concerns (Smith et al., 2011). Individual privacy has become important, even critical, for all of the organisations that handle individuals' personal information and data.

Although the term *privacy* has been researched for more than 100 years from different perspectives, such as philosophical, sociological, psychological and legal, the meaning of the

term is still in disarray. There is no one who can articulate what is really means exactly (Solove, 2006; Smith et al., 2011).

It is, thus, essential to define and understand the term *privacy*. This is necessary for two main reasons. The first is to help establish appropriate information security policies within the field of health services and for legal requirements, such as in the event of any dispute. There are many definitions of privacy in the literature. One of these definitions focuses on individual rights, in addition to moral and legal rights. Clarke (1999) is one of the researchers who defined privacy in this respect, stating the following: 'Privacy is often thought of as a moral right or a legal right' (p. 60).

Pavlou (2011) summarised privacy in simple terms, as his definition is based on how an individual controls how his or her personal information is acquired and used. He stated the privacy refers to

> "The concept of controlling how one's personal information is acquired and used"
> (Pavlou, 2011, 977)

Skinner et al. (2006) went further, as they defined privacy from the perspective that it is a human right. Clarke (1999) identified four main dimensions of privacy rights from the human right perspective. These dimensions include privacy of a person, individual behaviour privacy, individual communication privacy and individual data privacy. This research is mainly concerned with individual data privacy. Clarke (1999) defined information privacy as 'the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves' (p. 72).

On the other hand, Smith et al (1996) identified four additional dimensions of information privacy. These dimensions include improper access to information, collection, unauthorized secondary use and errors in managing information. Other classifications of privacy include information processing, information collection, information dissemination and invasion (Solove, 2006).

One of the main drives for introducing and implementing information security regulations and policies is concern for individual privacy. Malhorta et al. (2004) defined individual privacy concern as

> "An individual's subjective views of fairness within the context of information privacy"(p. 337).

One of the main findings of the literature of individual privacy concern is its role in, and influence on, individual attitudes towards privacy. These attitudes often play a major role in individuals' perceptions, practices and behaviours towards information security policies within an organisation. Attitudes towards privacy can include demonstrating sensitivity towards sharing and potentially losing personal information (Miyazaki & Krishnamurthy, 2002; Norberg & Horne, 2007). However, one of the main concerns of information privacy is that each piece of research in the literature conceptualises attitudes differently (Bélanger &Crossler, 2011).

Beldad et al. (2011) argued that the main challenge to organisation is the reality that people's attitudes towards the privacy of their own personal information are complex. He stated that individuals sometimes claim that they value the privacy of their personal information; however, they are often willing to trade this information for certain tangible or intangible benefits.

It is important to understand and acknowledge how privacy and security issues are related in practice. On the other hand, security corresponds to the organisation's concerns about the protection of personal information with three specific elements: integrity, confidentiality and authentication (Belanger et al. 2002; Camp, 1999; Smith et al., 2011)

From the information security point of view, an organisation can be considered successful in securing an individuals' stored personal data and information, but it could fall short regarding the subsequent use of personal information. This can lead to information privacy problems within the organisation operations (Culnan & Williams, 2009). Ackerman (2004) suggested that "security is necessary for privacy, but security is not sufficient to safeguard against subsequent use, to minimize the risk of private information disclosure, or to reassure users" (p. 432).

The distinction between privacy and confidentiality needs to be clarified. Privacy can be considered as a person's desire to control the disclosure of personal information. Confidentiality corresponds to the controlled release of an individual's personal information to an information custodian under a certain agreement that limits the extent and conditions under which such information may be used or released further (Smith et al., 2011).

2.4 Medical Information Privacy

It is important to stress and understand that medical information is highly confidential and contains private personal information and data. It can also be argued that even legitimate access to such information and data raises concern (Chen et al., 2012). This has led to health service authorities taking initiative towards information privacy. McBride (2008) argued that difficulties

facing the organisation in overcoming privacy concerns have contributed to organisations' taking initiatives to protect employees' and customers' privacy.

One of the main activities of health care services is the transmission of medical information with the health care stakeholder —for example, patients' medical information transmission between hospitals, wards and insurance companies. Therefore, the concerns of the privacy, integrity and confidentiality of a patients' data in the transmission process are not surprising. Health care service providers warned that patients' highly confidential medical information, such as diagnostic data results and type and severity of illness, could be breached during the information transmission process within the health care services activities. Furthermore, Clark (2008) also stressed the high-profile nature of data breaches of celebrities. The author argued that clinicians' unauthorised access to celebrities' medical information can represent a serious breach of the celebrities' privacy and can lead to serious legal disputes between the celebrity and the health care service provider.

Adesina et al. (2011) argued that the privacy, integrity and confidentiality of patients' medical data information represent the key factors to be considered in the data transmission process in health care service activities. They stated that the privacy, integrity and confidentiality of a patient's data are key factors to be considered in the transmission of medical information for use by authorised health care personnel (Adesina et al., 2011).

They argued that medical information sharing in the medical process is the vital issue of the authority's main concerns and that this should not be compromised by any means due to the seriousness of breaching patient's privacy.

2.5 Health Services and Electronic Recording

One of the main features of medical information in recent years is the implementation of technology in handling patients' and staff members' personal information. From the patient's point of view, electronic patient records have become central to the health services activities and functions and part of the reform strategy. Fetter (2009) argues that patient-centric personal health records (PHRs) are important, even critical, companions to health care services policies and strategies worldwide.

The introduction and the implementation of electronic recording is aimed at improving the quality of health care, reducing the cost of hospital operations and coordinating care. However, the implementation of electronic recording raises concerns regarding information security and the privacy of the medical information.

Williams (2013) argued that the main drives for introducing information security policy are the sharp expansion of e-health functionality, the need to comply with the national and international legislation and directives and the implementation of new medical technology in the hospitals' operations. Further, it is evident that health services worldwide are moving quickly towards the effective use of electronic recording. Saudi Arabia is in the process of introducing and implementing electronic recording through the Kingdom's health services. One of the worries and challenges of introducing electronic recording in the health services is the security of the electronic records. Fetter (2009) argues that the security of the health service data worries patients, health service providers and regulators.

2.6 Culture

The term *culture* is Latin in origin. The term means *ciltura* and *cultus* meaning care and cultivation. However the word reflects a variety of meanings (Kahler., 1968, p. 3.). It is difficult to find one generic definition of culture. Indeed, there are several definitions of culture in the literature— for example; Haralmbos et al. (2004) defined culture as "the whole way of life found in a particular society. It was suggested that culture can be learned and shared by members of a society"(p. 790).

The definition usually reflects the scholars' opinions and disciplines. Kidd (2002), for example, stated another definition of culture. The definition is similar to the above definition, as it is "the way of life of a group of people" (p.5).

Individuals within a society or an organisation behave in accordance with a set of values and norms. It can be argued that the values and norms are the main characteristics of individuals or groups, as these are examples of culture. Cultural value can be described as the end result that the individual behaviour patterns aim to achieve. On the other hand, the term *norm* can be defined as the prescribed ways or patterns of behaviours that a society expects of its 'normal' members (Kidd, 2002, p.17).

Hofstede (2001) explained culture by illustrating it as having four layers, in what the author referred to as the onion diagram. The core of the layers holds the values of the culture. It can be argued that a society or an organisation's values are the core of the culture. The author identified the layers of rituals, heroes and symbols, respectively. The symbol represents the surface layer of the onion diagram. The symbol of culture includes the fact that members of the same culture wear clothing and buy products that are typical of that culture.

2.6.1 National Culture

The role of national culture on the individual behaviour within the society is well established. Individuals develop a set of national values and norms that play a critical role in the individual's opinions and beliefs that may influence his or her behaviours and reactions to certain tasks. Therefore, it is important to define national culture. This is needed to help support the argument and discussions of cultural issues that are going to be used in this research. There are several applicable definitions of national culture, and usually, the definition reflects the author's background and experience. One of the well-established definitions is Hofstede's definition, which is "the collective programming of the mind that distinguishes the member of one group or category of people from another" (2001, p. 9).

Cultural analysis discussions and analyses can be understood by envisaging boundaries around each cultural group that shares the same culture. The boundary is an imaginary line needed to split the cultural groups from one another. Drawing boundaries between societies and studying their cultures can explain this. From the organisation's cultural point of view, a similar approach can be used to understand and analyse an organisations culture. It is important to stress that a society/organisation culture interacts across the boundary with other cultures. The interaction and flow of materials and values may influence culture over a period of time. Change in a society's values and norms, which are due to the impact of external cultural interactions, is referred to as "cultural contamination". Craig and Douglas (2006, p. 331) explained this change by stating the following: "One important consequence of changing cultural boundaries and the reconfiguration of the cultural context is cultural contamination. No longer can pure "ethnic" core of a culture and its distinctive compositional elements be clearly distinguished".

2.6.2 Hofstede's Dimensions of Culture

One of the most well-established and recognised studies of cultural dimensions in the literature is a Hofstede's dimension of culture. The dimensions are based on comprehensive research carried out on 72 countries between1967–1973. The research was based on a designed questionnaire that aimed to identify the dimensions of organisation culture. The research collected a total of 166,000 questionnaires from the surveyed countries (Hofstede, 2001, p. 41). The questionnaire responses were analysed based on theoretical reasoning and statistical analysis to explain the differences between the surveyed countries' cultures. The author identified, based on the survey, four main cultural dimensions: power distance, uncertainty avoidance, individualism and collectivism, as well as masculinity and femininity (Hofstede, 1980). A fifth dimension added to the four dimensions is based on a survey of Chinese national culture, Long-term vs. Short term Orientation Dimension (Hofstede, 2001).

Power Distance (PD) Dimension

This dimension is based on the suggestion that people in the society are unequal in status and social power. Hofstede argued that power is distributed unfairly in any society. This creates a distance and/or gap in the power within the society. Power distance can be defined as "a measure of the interpersonal power between boss (B) and subordinate (S)"(Hofstede, 2001, p. 83). Mudler (1977, p. 90) has also explored the power distance in the society and argued that the power distance can be defined as "the degree of inequality in power between a less powerful Individual (I) and a more powerful other (O), in which (I) and (O) belong to the same (loosely or tightly knit) social system"

One of the concerns of Hofstede's dimensions is gender power within a society. This argument is based on the existence of the power distance between males and females within one society. This may depend on the society's national culture. Stedham (2004) argued that Hofstede's dimensions are gender-specific, with only one exception: masculinity/femininity. The author also argued that gender power distance exists in Japanese society. This needs to be considered when analysing Japanese culture. The gender power distance dimension can be critical in a male-dominant society, in which the power rests mainly in the hands of the male. In such a society, females have less power in the society and are controlled by males. From the Saudi Arabian point of view, the gender power distance may need to be considered in order to identify and establish the role and impact of male's power as being dominant on the society's social and cultural behaviour and in the decision-making process.

Uncertainty Avoidance (UA) Dimension

This dimension focuses on the level of stress in the society in the face of unknown and unexpected future events. This represents society's ability and willingness to embrace change and reluctance to cope and deal with ambiguity (Lucas, 2006). From the organisation's point of view, its culture can be influenced by unpredictable future events, such as sudden periods of recession or war.

Individualism vs. Collectivism Dimension

This dimension is distinguished between individual and group behaviour within the society. Hofstede (2001, p. 209) described this dimension by stating that it is "the relationship between the individual and the collective that prevails in a given society".

Individualism describes when people place their personal interests and goals ahead of those of the social group within the society. It emphasises that an individual's behaviour within the society is based on his or her own interest and goals, regardless of the group's interest and goals. Hofstede (2001) argued that the type of society, particularly whether it is organised from the point of view of individualism or collectivism, has an impact on the organisation's employees' reasons to comply with an organisation's policy and requirements. There are several elements influencing individualistic behaviour within an organisation. These factors include social norms, levels of education, organisation culture and organisation history (Hofstede, 2001).

One of the key issues explored from individual and collective perspectives is the role and impact of societal norms on the individual's relationship with the organisation. Hofstede, (1980, p. 217) stated "the norm prevalent in a given society as to the degree of individualism/collectivism expected from its members will strongly affect the nature of the relationship between a person and the organization to which he or she belongs".

One of the distinctions between individualism and collectivism is that individuals from cultures that adhere to collectivism show a greater tendency to cooperate in the organisation and society at large. They relate more to people within their cultural group, and they feel more part of the group (Cox, 1991; Wenger, 1995). On the other hand, individualists are considered more autonomous entities that are independent of their cultural group (Markus & Kitayama, 1991). Individualists tend to be more competitive in the work place when compared with collectivists, and they try to improve themselves based on their own personal interests (Redding, 1993; Wanger, 1995).

Masculinity vs. Femininity (MF) Dimension

This dimension can be argued as the only dimension that recognises the differences between male and female roles in a society. Seldham (2004, p. 239) described this dimension as "the degree to which gender roles are clearly differentiated within a country. In masculine countries, gender roles are very distinct and separated. Men are assertive and tough; women are modest and tender".

This dimension argued that males score significantly higher than females in emotional actions (Seldhom, 2004).

Long-term vs. Short term Orientation Dimension

This dimension was added to the original Hofstede dimensions, as based on the Chinese Value Survey (CVS) around the mid-1980s. This dimension is considered to be the fifth dimension of culture and is used to analyse and discuss cultural issues. The dimension is based on the teachings of Confucius, particularly on both of its poles' items. The dimension argues against the short-term aspects of Confucian thinking and thrift, and focuses on personal stability, respect and valuing traditions. Put simply, individuals value their historical tradition and values (Hofstede, 2001).

2.6.3 Leadership and Organisation Culture

An organisation's employees rely on the established system to protect their job. They provide little resistance, avoid any conflicts with management, and conform to such a system in an attempt to ensure their job security (Henderson, 2011). From health service employees' perspectives, nursing practices have a strong history of being task-focused due to the nature of the job activities (Pearcey, 2007). Ruighaver et al. (2007) explained that within an organisation, information security is primarily a management problem and how

management deals with information security is a direct reflection of an organisation's culture. Organisation leadership and management play a major role on developing and enhancing appropriate working culture, (Van Niekerk and von Solms, 2010; Chang and Lin, 2007; Kritzinger and Smith, 2008).

One of the organisation culture's frameworks is the basis of truth and rationality. The basis of truth and rationality is the first component of the organisational culture framework, and it refers to the truth in security beliefs and actions.

2.7 Information Security Culture

Aside from the use of technology, humans themselves play a major role in managing and controlling health care services information. Over the last few decades extensive research and development has been conducted in using technology to protect health care information by strictly controlling access to the information, using technology such as specific usernames and passwords. Technology also helps to categorise information and users into groups based on their jobs' roles and responsibilities, and this will help protect information. Another concern is the role humans play in healthcare service information security. The role of humans in information handling is consistently referred to as the weakest link in information security (Huang et6 al. 2007; Huang et al., 2009). Schulz (2005) argued that information security is not a technical problem or issue that needs to be considered but that it concerns people, and this needs to be considered carefully by information management authority members.

One of the issues raised in the literature regarding the role of people considers users' awareness and understanding of what being 'secure' actually means (Lacohee et al., 2006). This may be due to a lack of training and educational programmes regarding information security. Chan et al.

(2005) indicated that one of the main causes of concern and challenges in an organisation is that its employees often fall short in complying with information security policies and guidelines. It is important to stress that maintaining an organisation's information security is not only the responsibility and duty of the information technology specialist within the organisation, but it is also the duty and responsibility of all of the employees within the working environment of the organisation (Rotvold, 2008, p. 33). The author argued that information users need to be aware of their exact roles and responsibilities in protecting the information and those they should respond by taking appropriate actions and measures when dealing with any potential security issue.

Several authors stressed clearly that an organisation's information security problems are evidently linked to its employees' behaviour (Thomson et al., 2006; Siponen and Oinas-Kukkonen, 2007; Workman et al., 2008).

Technical controls can provide substantial protection against many of these threats, but they do not provide a comprehensive solution (Rotvold, 2008, p. 33).

These technological methods of protecting information may be partially effective. However, many losses are not caused by a lack of technology or faulty technology but rather by users themselves and faulty human behaviour (Rotvold, 2008, p. 33)

Patnaik, (2011) carried out a study to understand the role of the organisational working culture on enhancing organisational health. Organisational health refers to "an organisation's ability to achieve its goals based on an environment that seeks to improve organisational performance and support employee well-being" (Patnaik, 2011, p.43). Spiers

(2003) argued that the UK's NHS must have the potential to overcome organisational culture issues in order to be able to respond efficiently and effectively to patients' needs, and expectations.

Worthington (2004) examines in-depth concepts of cultural management in the NHS. The author argued that organisational change requires change in the organisation's culture to avoid any tension and conflict within the organisation.

Young (2007) stressed that the organisation's dominant groups' power within the organisation are the groups who control and manage its resources and set the rules.

Martin (2002) observed the organisation's political, power and conflict tension are associated with organisation culture. Burke (2002) stressed that individual behaviour within the organisation is driven by the individual employees' needs and values. He argued further these also play a major role in individual employees' motivation. The author establishes the link between the employees' values, needs, belief and organisational congruence. Schein (2010) highlighted that organisation culture is open to change.

Currie and Lockett (2007) argued that moral and ethical considerations are the main drives for leadership. They argued in favour of 'transformational leadership,' where politicians ought to focus on realising public opinion for the delivery of a quality health service.

Robbins and Judge (2008) argued that nursing working culture is changing due increased bureaucracy across the NHS and this has led to formulated rules and regulations.

Dickson and Smith (2013) concluded that transformational and transactional leadership at all levels of the organization need to work together to ensure effective change in health services. They argued that organisational culture needs be considered carefully during organisational change.

Campbell and Goritz (2014) investigated corrupt organizational culture from the perspectives of organizational values and norms. The investigation was based on qualitative data analysis, and in-depth interviews with key experts on organizational corruption. They found that security and punishment of deviants is an important and valued norm of the corrupt organization. They also found differences between employee and management perception towards culture.

Jung and Takeuchi (2014) compare national culture differences between employees, organizations, and work attitudes in Japan and Korea. They used 138 Japanese and 144 Korean employees in the private sector. They found that national culture plays a an important role in work attitude.

Engelen et al. (2013) showed that national culture plays a major role in organizational culture due to strong individualism and power distance in advancing entrepreneurial orientation and it represents a major problem for entrepreneurial orientation.

McGuire et al. (2008) argued that organisation culture has a significant influence on organisational performance. They argued that organisation culture contains a system of beliefs that require certain behaviours and exclude others. It sets norms on everything in the organization.

McGuire et al. (2008) stressed that organisational change requires senior leadership acknowledging their role in the cultural change process.

Schmiedel et al. (2014) identified organisation culture as one of the main elements of Business Process Management (BPM) needed to enhance organisation effectiveness and efficiency.

Watson (2006) emphasised the importance and need to create a strong organisational culture through management thinking and strategy.

Zalami (2005) noted that organisational culture can either facilitate or inhibit the organisation's success in achieving its goals.

Schein (2004) highlighted the responsibility of the organisation's leaders to create an appropriate culture and develop a positive and productive culture through their understanding of the organisation.

2.8 Information Security Policy

In Europe and North America, several steps have been taken to protect information and data from any unauthorised access and use. The European Union Data Protection Directive requires the implementation of technical and organisational measures in the design and operation of information management systems and use of information and communication technology, ICT (Rubinstein, 2011). However, the author argued that this has been proven insufficient to protect information and argued for increased privacy protection by designing a specific approach. Privacy by design can be achieved by adopting two main approaches. The first approach incorporates substantive protection into the organisation's operational practices, and the second approach is to maintain and control comprehensive data management procedures throughout the organisation's services and products' life cycles (Rubinstein, 2011).

Muhaya et al. (2012) identified five layers of information security issues. These issues include security policy issues in the environment layer, security policy issues at the application layer, cryptography policy issues, security policy issues at the network layer and security policy issues at the infrastructure and physical layer. The main issues related to this research are the security policy issues at the environment layer. The main issues identified at this layer include an

organisation's employees' awareness, training and readiness, as well as their attitudes towards information security. Gregory et al. (2007) identified that employees' awareness towards information security issues and implementation of the organisation's information security should be considered in securing an organisation's information within its working environment. Therefore, organisation management needs to ensure employees' awareness of their strategic planning in protecting information and ensuring secure information management and control. One of the approaches that can be adopted by management to promote employees' information security awareness is through implementing effective and well-planned training courses and educational programmes. Training in technology is identified as an important approach in promoting and enhancing information security (Muhaya et al., 2012). Adams et al. (2005) identified that the communities' practices in their working environments play an important role in promoting and supporting the implementation of information security. Therefore, it is not surprising information security policy has become an important part of organisation management plan and strategy, (Kolkowska and Dhillon 2013; Knapp, et al., 2009).

2.9 Behaviour towards Technology: Accepting Technology Models

One of the well-established models on human behaviour is the accepting technology model. There have been many studies in this area in the last few decades due to sharp changes in the use of technology and e-learning. From this research perspective, the model investigates and analyses human behaviour based on the individuals' attitudes towards taking action. Davis et al. (1989) presented a well-recognised model in the literature for human behaviour towards accepting technology, Technology Acceptance Model, TAM.

Figure 6.1 shows the technology acceptance model. The model is based on two constructs: ease of use, and technology's influence on the individual's attitude. The model states that the individual's attitude towards technology plays a major role in the intention of the individual to actually use the technology. Intention of usage can lead to actual behaviour—i.e., the actual usage of the technology.

From an information security point of view, it can be argued that individual employees' attitudes can lead to the individual intention to use information, and the intention to use information can lead to actual use of information.

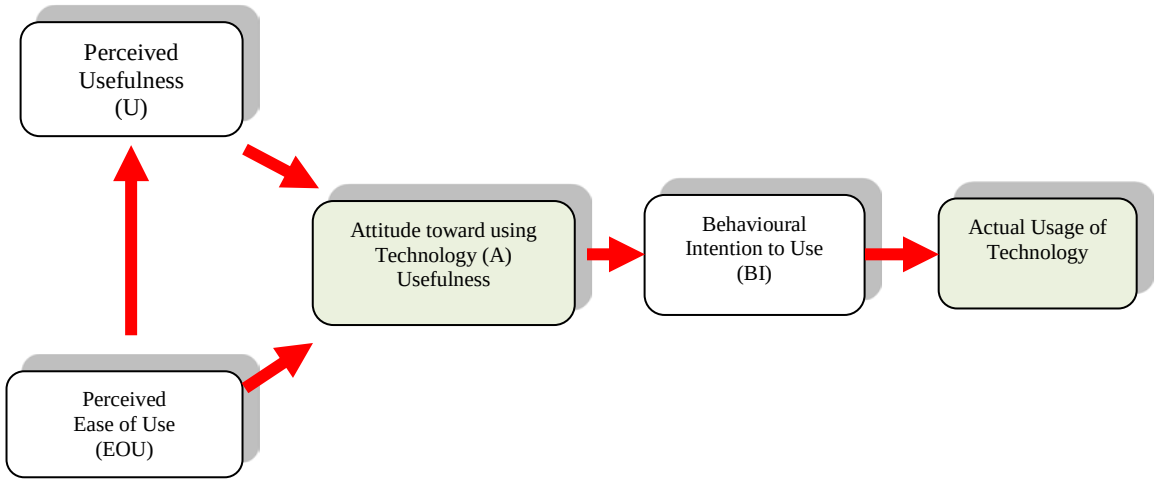

Figure 2-1: Technology Acceptance Model, TAM (Davis, 1989)

2.9.1 Theory of Reasoned Action (TRA)

The theory was developed and argued for by Ajzen and Fishbein (1979). Figure 6.2 shows the TRA model. The model is based on the fact that the individual's attitude and behaviour are derived from individual beliefs and evaluations of required actions. The attitudes developed play a major role on the individual's intention to take action. The model also suggested that normative beliefs and motivation lead to a subjective norm (SN). The subjective norm plays a role in the individual's inclination to act, e.g. buying a product or using e-learning resources. Again, behaviour intention leads to actual behaviour.

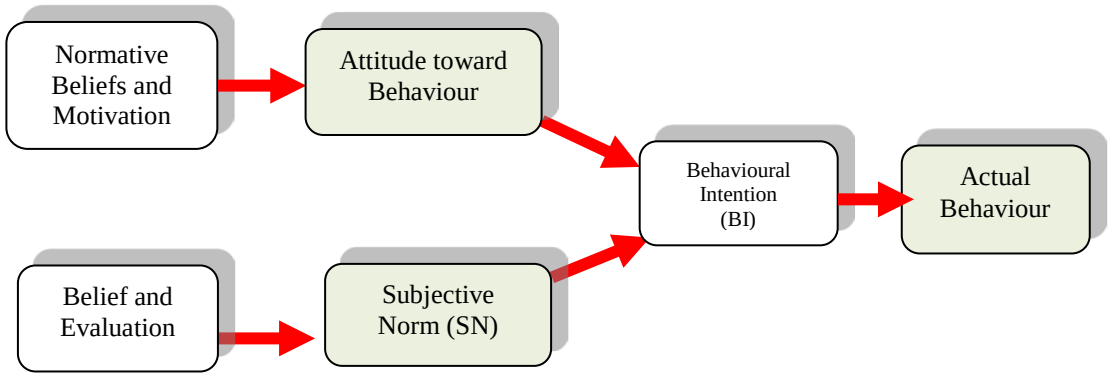

Figure 2-2: Theory of Reasoned Action (TRA) (Ajzen & Fishbein, 1980)

2.9.2 Intrinsic and Extrinsic Motivators in Information Security Behaviour

Herath and Rao (2009) developed the information security behaviour compliance model. The model is based on intrinsic and extrinsic dimensions that influence an individual's intention to comply with the information security policy, and intention to comply leads to actual compliant behaviour. Extrinsic motivation dimensions include penalties and social pressure for employees' compliance with information security. The social pressure for compliance includes peer behaviour and normative beliefs. Positive peer behaviour towards compliance of information security policies can be one of the social pressures that contribute to the employees' intention to comply with the policy. Normative belief is the individual's perception about information security policy compliance, which is influenced by the person's parents, spouse, friends and relatives. The penalty dimension includes the severity of the penalty for not complying with the policy as well as the certainty of detection. On the other hand, the intrinsic motivation dimension includes the perceived effectiveness of penalties for policy compliance.

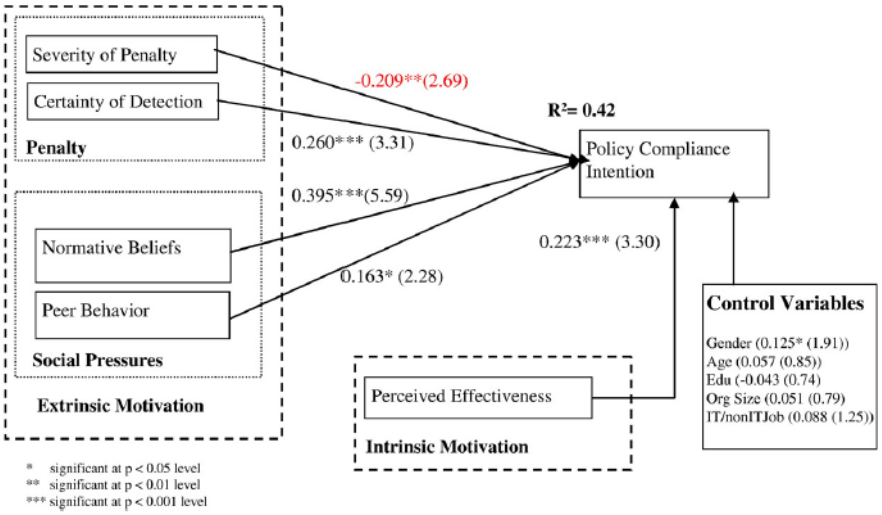

Figure 2-3: Intrinsic and extrinsic motivators in information security behaviours (Herath & Rao, 2009)

2.10 Summary

The main outcomes of this literature review can be summarised as follows:

- Employees' attitudes towards information security are the main issues for effective implementation of information security policies (Muhaya et al., 2012).
- Employees' understanding and awareness of the information security issues and their implementation of information security policy play an important role in protecting an organisation's information (Gregory et. al. 2007)
- There are several information security culture dimensions explored in the literature. These dimensions include organisation leadership, trust, national culture and technology

CHAPTER 3
RESEARCH METHODOLOGY

Chapter 3 Objectives

The main objectives of this chapter are as follows:

- To provide justification for the data collection methods;
- To clarify and state the research samples;
- To clarify and justify two fieldwork data collection visits;
- To discuss and present the questionnaire and interview structure;
- To introduce and justify a pilot study.

Chapter 3 **Research Methodology**

3.1 Introduction

Chapter 1 of this research presents the background of Saudi Arabia's National Health Service. The background shows that the Saudi Arabian National Health Service has seen a sharp expansion in the last few decades. There are many SA national health services competing in the market. There is a lack of data and information on the roles and impact of culture on Saudi Arabian national health services. This chapter introduces the research methods that will be adopted to achieve the research aims and objectives. The chapter presents the main research philosophy and strategies. These help the researchers to understand the principles of the research and the way that the research can be carried out. The chapter also presents the data collection methods that will be adopted in collecting both quantitative and qualitative data. The chapter closes by identifying the appropriate data analysis that will be used when analysing the data.

One of the main steps in the research process is to identify an appropriate research strategy. Yin (2002) explored five different research strategies. These strategies are the experiment strategy, the case study, the survey strategy, archival research and the historical research strategy. After careful consideration, we determined that the survey is the most appropriate strategy for this research. This is mainly due to the nature of the research. Survey strategy can be defined as a "system for collecting information from or about people to describe, compare, or explain their knowledge, attitudes, and behaviour", (Fink, 2003, p. 1).

The use of the survey strategy in this research helps in providing quantitative and qualitative data for describing the research subject trends, perceptions and attitudes towards the main issues in the research.

The main objectives of the research methodology can be summarised as follows:

- To identify and justify the research methodology;
- To identify and justify data collection methods;
- To identify and justify the research sample;
- To plan pilot study for the questionnaire and the interviews.

3.2 Adopted Methods to Answer Research Questions

This section presents and discusses the primary adopted methods to answer the research questions.

3.2.1 Literature Survey

The first step in this research is to critically review the related literature. This is needed to develop the initial framework of the research and to benefit from other research related to the research topics to cover the research objectives.

3.2.2 Data Collection

The research adopts a multiple methodological approach to collecting data. This includes collecting quantitative and qualitative data to support outcomes analysis. This type of approach helps in providing data and information from different resources to achieve the research's aims and objectives as well as in answering the main research questions (Denscombe, 1998; Sekaran, 1992). The mixed approach used in this research includes collecting qualitative and quantitative data. Data from the research fieldwork—namely, Saudi Arabian health services—is needed to provide raw data that can be used to identify and explore the current information security culture in the service and to explore the main challenges in promoting and enhancing information security culture. The data collection process will be done in two stages. The first stage is aimed at providing raw data and information to help develop the information security model culture. This stage involves distributing a semi-structured questionnaire to three main hospitals in Saudi Arabia. This stage also involves conducting in-depth, face-to-face interviews with key personnel of the three hospitals to explore key personnel members' opinions and attitudes towards information security culture as well as the main factors

influencing their information security culture. The main purposes of the interviews are to explore and identify information security culture to help with developing the initial information security culture model, (Walsham, 2006; Marschan-Piekkari and Welch 2004). The main outcomes of this stage combined with the outcomes of the literature review helped in developing the initial information security culture model. The developed model is needed to achieve the research objective.

3.2.3 Modelling

Developing an information security culture model is one of the main objectives of this research. The developed model will be discussed in greater detail in Chapter 7. The purpose of the model is to provide the SA health authority figures with a model that helps in developing and enhancing their information security culture strategy and policy. The model has been developed based on two main outcomes. The first outcome entails the main findings of the data analysis of the first survey on the SA health services, which are listed in Chapters 5 and 6, and the second includes the main findings of the literature survey in Chapter 2.

3.2.3.1 Develop and Design Information Security Culture Model

The model has been developed and designed based on a set of cultural dimensions identified and explored by the survey data analysis and the literature survey. The model consists of cultural dimensions and sub-dimensions that influence the health services' information security cultures and the employees' attitudes towards information security behaviour. The model identifies and relates the role of the cultural dimensions and the sub-dimensions to the hospital culture and the behaviour of the staff towards information security culture. The information security culture

helps in developing the information security culture policy, and this will be discussed in the next section.

3.2.3.2 Develop and Design Information Security Culture Policy

Health service employees' behaviours and the organisation's culture play critical roles in hospital information security, which includes the patients' medical records and staff personnel details. Therefore, there is a need for a clear and effective hospital policy to establish and clarify the expected interactions and behaviours towards information security. The model of this section aims to develop an information security policy within a cultural context, as the technical aspects can be argued to require better grounding in research. The SA health authority requires a framework model for developing an effective information security culture policy to protect the patient's medical records. The policy model is based on the main outcomes of the first model—namely, the information security model. The policy takes into consideration the cultural dimensions and the staff members' attitudes and behaviours towards the information security model. This model will be discussed in detail in Chapter 7 of this research.

3.2.3.3 Evaluation Process

The developed model presented in the previous sections needs to be evaluated to ensure its applicability, usefulness and practicality to SA health authority members. The evaluation of the model will be based on a second survey, on the research fieldwork of the Saudi Arabian health service. The second survey will collect quantitative and qualitative data by using the same survey that the hospitals used to evaluate the developed models.

3.3 Work Packages

The project plan is to be achieved through the completion of six work packages. The work packages plan is needed to manage the project time and tasks efficiently and effectively. The research is based on the completion of six work packages, which reflect the research's main aims and objectives. The work packages are presented briefly in the next sections.

Figure 3.1 shows the research plan with all research packages. The plan clearly shows the starting point of the research is to establish clearly the research aim and objectives. Once the research aim and objectivise clarified work package one is needed, namely the critical review of the literature. This package is needed to build understanding the project, increase awareness of other researches in the area and to develop the research framework. This package will be presented in the following section. Work package three is the research methodology. This is needed to clarify and justify research strategy adopted the data collection methods needed, and the sample of the research. Work package four is the data analysis and work package five is enforcing the developed model. Work package six is to establish the project main findings, conclusions, recommendations and suggestions for future work.

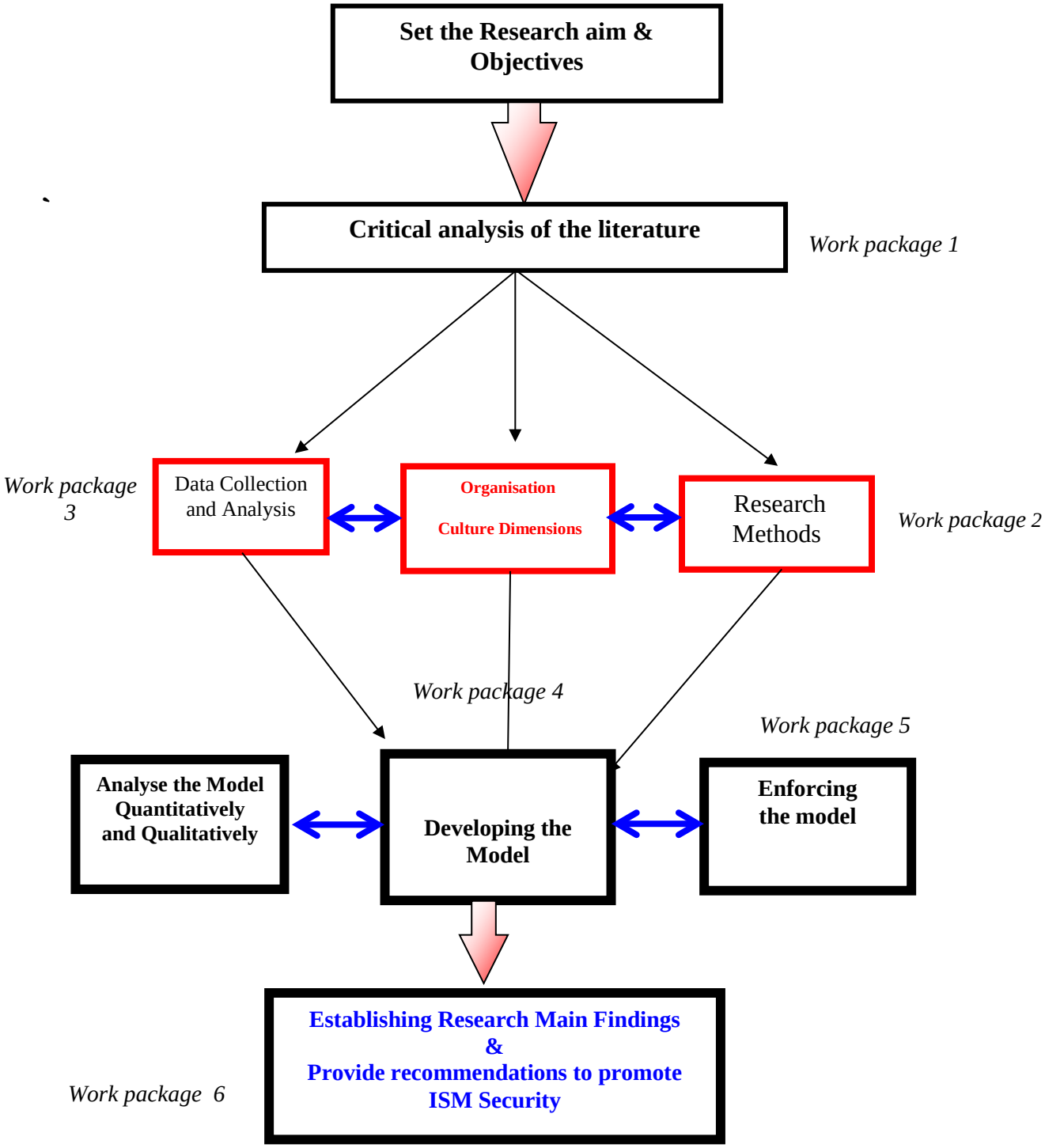

Figure 3-1: Research Plan

3.3.1 Work Package 1: Critical Review of the Related Literature

This package purpose is to review the related literature and focus mainly on the health service culture and, in particular, the information security cultural dimensions and the hospital's information security culture. This package is needed to help establish the research framework, enhance awareness of other research on the topics and enhance knowledge and understanding of the research topic. This package is presented in Chapter 2. The main outcomes of this package will be used in the next packages of the research process—namely, in developing an information security culture model and an information security culture policy model.

3.3.2 Work Package 2: Scoping the Research Methods

This package objective includes establishing an appropriate research method, scoping the research and hypothesis, and collecting data from Saudi health services to identify the current culture-related information security dimensions, barriers and problems. The research methods are presented and discussed in this Chapter. The package also includes designing a survey strategy for collecting quantitative and qualitative data from the SA health service. This includes designing, piloting and distributing a semi-structured questionnaire. The questionnaire focuses on the key personnel of SA health service staff. The package also includes designing, piloting and carrying out face-to-face, in-depth interviews with key personnel of the selected hospitals. The task of data collection is to identify and explore the information security cultural dimensions as well as related information security culture problems and obstacles.

3.3.3 Work Package 3: Data Analysis

This package objective includes analysing the collected data and articulating the findings. The qualitative data as well as the in-depth, face-to-face interviews will be analysed manually based on the research's main themes. The main outcomes of this analysis are presented in Chapter 5. On the other hand, the quantitative data will be analysed using SPSS due to the nature of the data, (Pallant, 2005).

3.3.4 Work Package 4: Modelling

This package objective includes establishing the research framework model and analysing the model quantitatively and qualitatively. The package includes two models. The first model is related to the information security model culture. The purpose of this model is mainly to relate the main cultural dimensions that influence a hospital's information security culture and the staff members' behaviours towards the information security culture. The model also identifies the most influential dimensions on the information security culture. The second model, (part of the first model), the information security culture policy model, was developed based on the main outcomes of the first model as well as on the outcomes of the literature survey and the collected data. This package is presented in Chapter 6 of this research.

3.3.5 Work Package 5: Enforcing the Developed Model

This package objective includes establishing a mechanism to enforce the developed model. This mainly entails providing a practical solution to enforce the model.

3.3.6 Work Package 6: Establish the Research's Main Findings

This package is mainly to establish the main findings of the research based on the data analysis and developed model. The package is also intended to identify the main cultural dimensions that influence information security in health services at the individual level as well as individual behaviour regarding information security at the organisational level.

3.4 Data Collection Methods

This section presents the analysis of the role and impact of hospital management on the hospital's information security. It is important to stress that the Saudi national health services are public services with limited private hospitals in the Kingdom. Their operations include managing the hospital budget, medical staff recruiting, strategic planning and enforcing policies.

3.4.1 Quantitative Data: Semi-structured Questionnaire

Quantitative data is needed in this research in order to provide numerical data to investigate and analyse Saudi Arabian National Health Service as well as perceptions and attitudes towards the role and impact of culture on the organisation regarding management performance. This type of data can be used to survey a large number of the SA National Health Service population.

A semi-structured questionnaire has been used in this research because the questionnaire can survey a large number of subjects. This is relatively cheap to carry out, and with a reasonable amount of time and effort, (Newman, 2006). The participant can complete the questionnaire at his or her own convenience. The main disadvantages of the questionnaire are that the

participants cannot express their views freely and that there is no any way to test the truthfulness of the respondents.

3.4.1.1 Semi-structured Questionnaire Design

This project's researchers have designed a semi-structured questionnaire to identify the current problems in SA hospitals, which is located in Appendix A. The questionnaire has been designed for the Saudi Arabia National Health Service to identify the industry employees' opinions and perceptions towards the role and impact of culture on information security. Both open-ended and closed-ended questions have been used in this questionnaire design. This is necessary in order to benefit from two types of questioning. In open-ended questions, the participant is permitted to express his or her views freely. On the other hand, the closed-ended questions are intended to direct the participants towards specific issues, (Creswell, 2003; Frazer and Lawley, 2000). The questionnaire has five sections, each with a set of questions. The sections are as follows:

Section A: Personal Details

Section B: Leadership Style in the Organisation Management

Section C: Hospital Culture

Section D: Hospital information security policy culture

Section E: Role of National Culture

3.4.1.2 Questionnaire Distribution

The designed questionnaire, Appendix A, will be distributed to the three selected Saudi Arabia National Health Service hospitals. The questionnaire will be distributed with a self-

addressed envelope to enable responses. The questionnaire will be distributed in-person with the help and support of the three organisations.

3.4.1.3 Semi-structured Questionnaire Sample

The National Health Service in Saudi Arabia are extensive, and it would be difficult to survey the entire Saudi national health service population. Therefore, it is important to carefully identify a sample that would accurately represent the entire Saudi Arabian National Health Service. Fink (2003, p. 1) defines a research sample as "a portion or subset of a larger group called a population".

Semi-structured Questionnaire Sample

It is important to select an appropriate sample process to collect reliable data and to avoid any biases in the data collection process. The literature has identified several sampling methods. These samples include simple random sampling, systematic sampling, stratified sampling and clustered sampling (Robertson & Dearling, 2004). Simple random sampling has been used in this research by giving all of the selected organisations' subjects' equal opportunities to select the interviewees. The interviewees are selected equally from the three selected organisations. Simple sampling has also been used, as the three selected organisations are located in one city. Table 3.2 shows the questionnaire sample from the three hospitals.

Table 3.1: Semi-structured sample and number of received questionnaire

	Hospital	Sample	Received
Semi-Structure questionnaire	King Faisal Specialist Hospital and Research centre	300	212
	King Fahad Medical City	300	208
	Specialised Medical Hospital	200	138
Total		**800**	**558**

3.4.1.4 Semi-structured Questionnaire Pilot Study

The designed questionnaire, questionnaire distribution and analysis all require significant time and effort. These steps also incur significant financial costs. Therefore, it is important that the questionnaire design is tested and evaluated well before its actual distribution to the research population. It is critical to carry a pilot study to evaluate the designed questionnaire in this research. One of the main purposes of the pilot study is to ensure the appropriate wording of the questionnaire. As Oppenheim (1968, p. 26) stated, "Pilot work can be of the greatest help in devising the actual wording of questions, and it operates as a healthier check, since fatal ambiguities may lurk in the most unexpected quarters".

In this research, a sample from within the Saudi Arabian National Health Service was selected to participate in the pilot study. Table 4.3 shows the main sample for the pilot study. The table also provides justifications for the sample selection. The pilot study selected five subjects from SA NHS. The sample size is reasonable and manageable with the possibility of creating a focus group following the completion of the questionnaire to reflect on the questionnaire's design and questions. Two subjects from SA NHS were selected for the pilot study, as the interview targeted the SA NHS.

Table 3.2: Questionnaire pilot study sample size and justifications

	Sample Size	Targeted Sample	Reasons
Semi-structured questionnaire	**5**	Saudi National Health Services	To ensure wording and structure of the semis-structured interviews
Semi-structure Interviews	**2**	Saudi National Health Services	To ensure wording and structure of the semis-structured interviews

3.4.2 Qualitative Data: Semi-structured Interview

Qualitative data is needed in this research in order to provide in-depth information to explain information security culture. This is critical in this research due to the nature of the research topic. Cultural issues need to be explored in-depth to support the research's main findings. One of the main advantages of carrying out face-to-face interview is that these interviews will assist the researchers in exploring and understanding complex cultural issues (Sekaran, 1992). This is needed in this research, as cultural issues are one of the main topics of the research. The interviews can be used to enhance the usefulness of the quantitative data, questionnaire analysis. The face-to-face interview will also use a semi-structured interview approach. Structured interviews are not appropriate for this research due to the need to give the interviewees the opportunity to express their opinions and perceptions towards the cultural issues freely based on their experience, knowledge and understanding and to collect statements from the interviewees' opinions and perceptions (Drever, 2003). In addition, the interviews need to focus on the research topics, which is why semi-structured, face-to-face interview will be used.

3.4.2.1 Interview Design

The face-to-face, semi-structured interviews were designed by establishing set of three main issues, and each issue features three questions; see Appendix B. The same questions and wording will be used in all three interviews to ensure fairness and reliability of the data (Patton, 1987). The three main issues are listed as the following three sections:

Section A: Information Security Policy

Section B: Role of Hospital Culture on Organisation Management

Section C: National Culture and Organisation Management

3.4.2.2 Interviewed Subjects Sample

The semi-structured interview designed in this research aims to explore and discuss the opinions and perceptions of key management subjects in Saudi Arabian National Health Service on the role and impact of culture on the SA NHS management performance. Two senior managers were selected from each organisation. There are 24 interviews in total. The low number of interviewees is mainly due to time constraints as the researchers need to meet the research submitting deadlines. Table 3.4 shows the semi-structured interview sample, selected organisations, a sample of the interview and the position of the selected interviewee. The three SA NHS hospitals were selected due to the organisations' sizes and establishment in the SA and international market.

Table 3.3: Interviews sample

	Organisation	Sample Size	Position of the interviewee
Semi-Structured Interviews	**King Faisal Specialist Hospital and Research centre**	8	2 Managers (Head of Department/Sectio
			2 Physicians
			2 Nurses
			1 Administrator
			MIS Member
	King Fahad Medical City Hospital	8	2 Managers (Head of Department/Sectio
			2 Physicians
			2 Nurses
			1 Administrator
			MIS Member
	Specialised Medical Centre Hospital	8	2 Managers (Head of Department/Section
			2 Physicians
			2 Nurses
			1 Administrator
			MIS Member
Total		**24**	

3.4.2.3 Interview Pilot Study

A pilot study for the designed interview was carried out to assess the clarity of the questions to the interviewees as well as to determine whether the response reflects the purpose of the question and the interviews.

3.4.2.4 Documentation Analysis

SA health service and hospital information security documents were analysed to identify and explore the current state of such documentation from the perspective of the information security culture. The document analysis includes the annual reports of information security and its investment in promoting and enhancing information security culture, the hospital's information security policy and the daily procedures and activities.

3.5 Data Analysis

The collected data needs to be analysed to provide results that can be used to support the research and to argue the main findings regarding information security culture dimensions. The quantitative collected data will utilise SPSS in the analysis process. Different statistical tests will be used based on the main variables of the questionnaire design. This many include frequency, cross tapping, standard deviation. These statistical methods are needed to achieve the research aims and objectives. The qualitative data and semi-structured interviews will be analysed manually based on the research issues. Finally, the data analysis results will be used in the research discussions.

3.5 Summary

This chapter has identified and justified the research methodology, data collection methods used, research sample, plan for a pilot study for the questionnaire of the research. The chapter also provided the work packages adopted in this research. The next chapter will use this chapter guidelines and tools to analyse the data collected from the field work.

CHAPTER 4
DATA ANALYSIS: QUANTITATIVE DATA ANALYSIS

Chapter 4 Objectives

The main objectives of this chapter are as follows:

- To analyse the collected questionnaire using SPSS as a tool in the analysis process; and
- To identify the main information security culture dimensions and sub-dimensions.

Chapter 4 **Data Analysis: Quantitative Data Analysis**

4.1 Introduction

One of the main aims of this research is to identify the primary cultural dimensions of the information security culture on Saudi health services. Therefore, it is important to collect data from the Saudi health services to reflect the reality of the current information security culture and to help develop a framework that reflects the Saudi health service culture. The focus of this research is on information security culture. This requires analysis of the SA health services. This section presents an analysis of the quantitative data. The analysis is based on designed questionnaires distributed to individuals employed in SA health services. The analysis is aimed at identifying the current information security culture issues and the main cultural dimensions. The analysis is needed to help develop an initial information security culture model for SA health services.

4.2 Survey Participants

A total of 800 questionnaires were distributed to three main hospitals in Saudi Arabia. We received 588 valid and completed responses. The majority of the responses were from King Faisal Medical City Hospital, (212 out of 558) 38% and 37% from King Fahad Medical City Hospital (208 out of 558) as shown in Figure 4.1. Although, the results analysis is specific for these three hospitals, the three hospitals represents the sample for the Saudi Arabia hospitals.

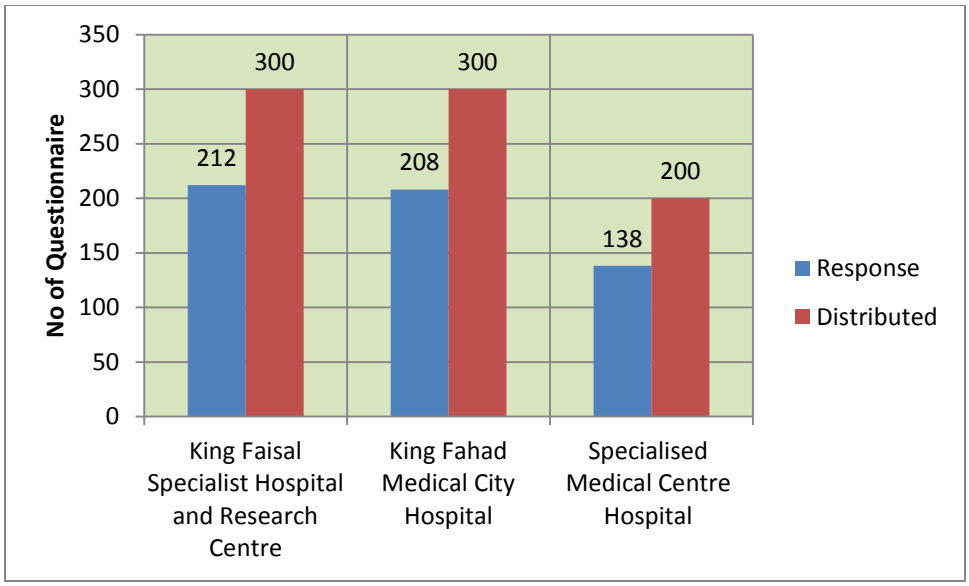

Figure 4-1: Surveyed hospitals

Figure 4.2 shows the gender of the participants and illustrates that the majority of the responses are from males (364 out of 588).

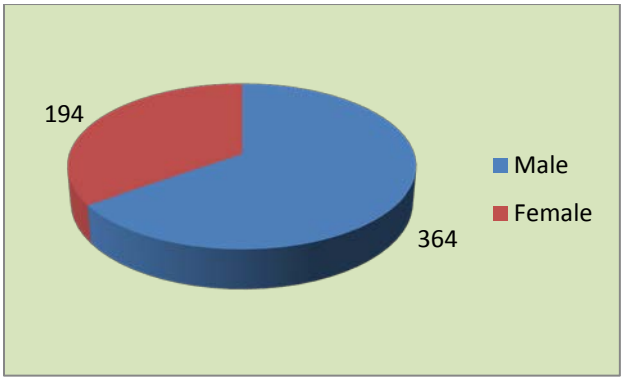

Figure 4-2: Gender of participants

There are several disciplines needed in health care services to provide appropriate care to patients. Disciplines depend on job roles in the care process. The vast majority of the respondents were residents (168 out of 558) and nurses (144 out of 588); see Figure 4.3.

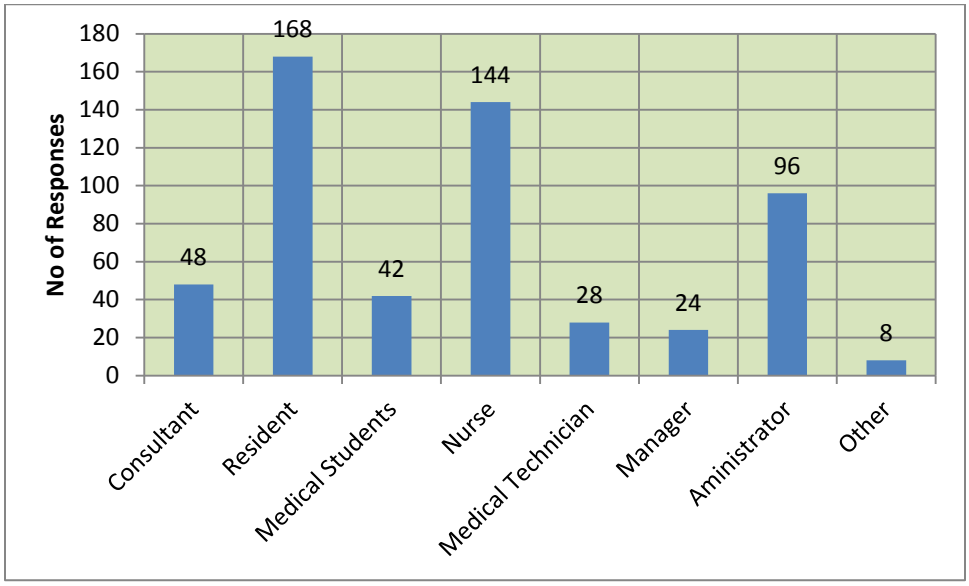

Figure 4-3: Discipline of the participants

Figure 4.4 shows the participants' experiences and illustrates that the majority of the responses have between 5–10 years' experience (192 out of 588), and only 42 out of 558 have over 25 years of experience.

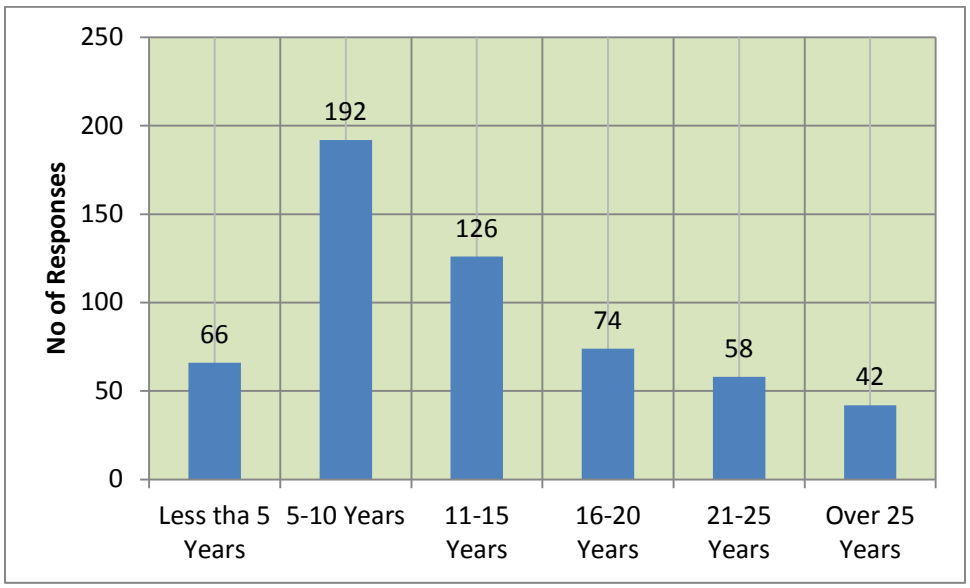

Figure 4-4: Participants' experience

4.3 Leadership Styles in the Organisation Management

Figure 4.5 shows the responses to the following statement: 'Hospital leadership creates an information security environment where the employee takes ownership of his or her tasks'. The vast majority, 367 out of 588, strongly agreed or agreed with the statement, and only 138 out of 558 strongly disagreed or disagreed.

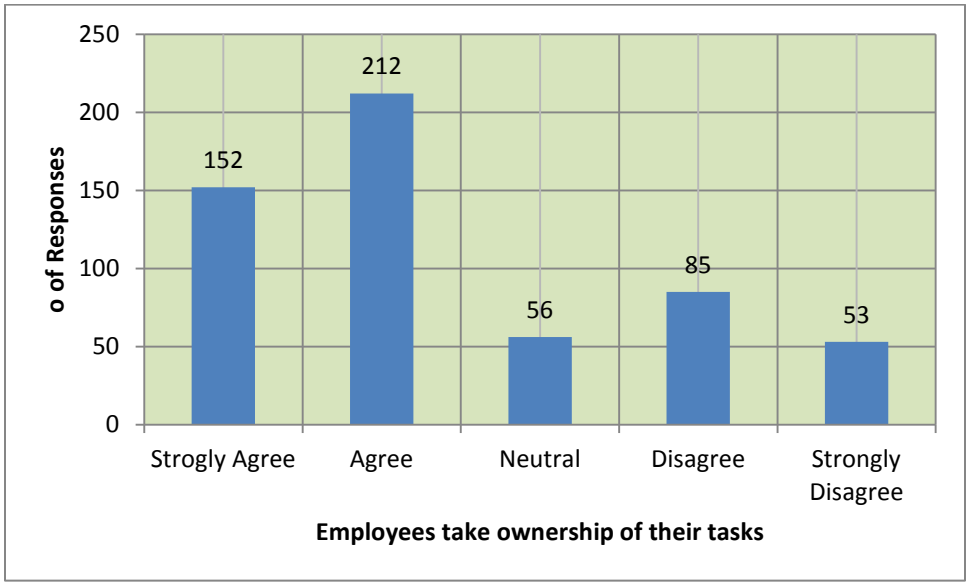

Figure 4-5: Leadership creates an IS environment that encourages ownership.

Figure 4.6 shows the responses to the following statement: 'Hospital asks employees for their vision of where they see information security going and then uses their vision where appropriate'. The vast majority, 424 out of 588, strongly agreed or agreed with the statement, and only 88 out of 558 strongly disagreed or disagreed.

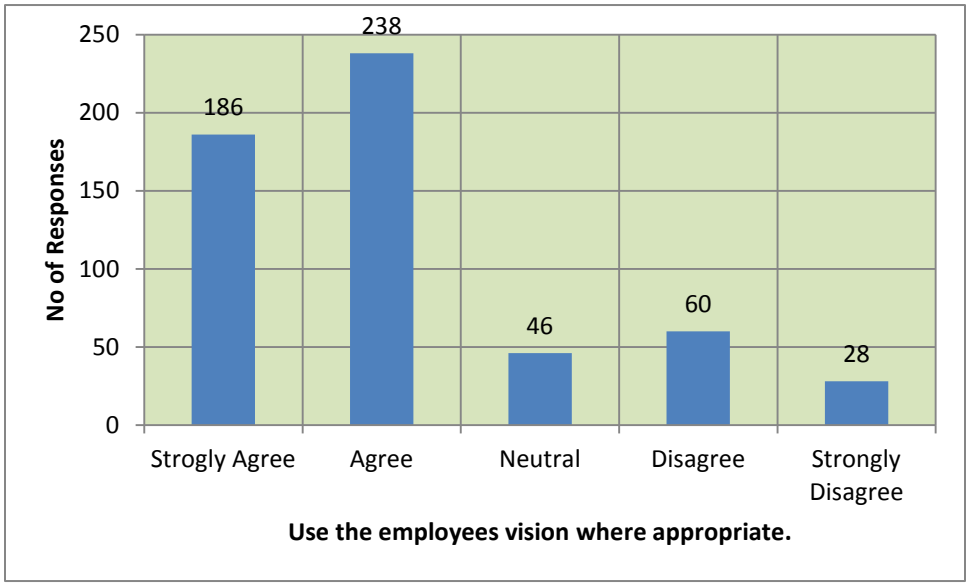

Figure 4-6: Hospital asks employees for their vision.

Figure 4.7 shows the responses to the following statement: 'Hospital delegates tasks in order to implement a new procedure or process in the in hospital'. The vast majority, 238 out of 588, strongly agreed or agreed with the statement, and only 182 out of 558 strongly disagreed or disagreed.

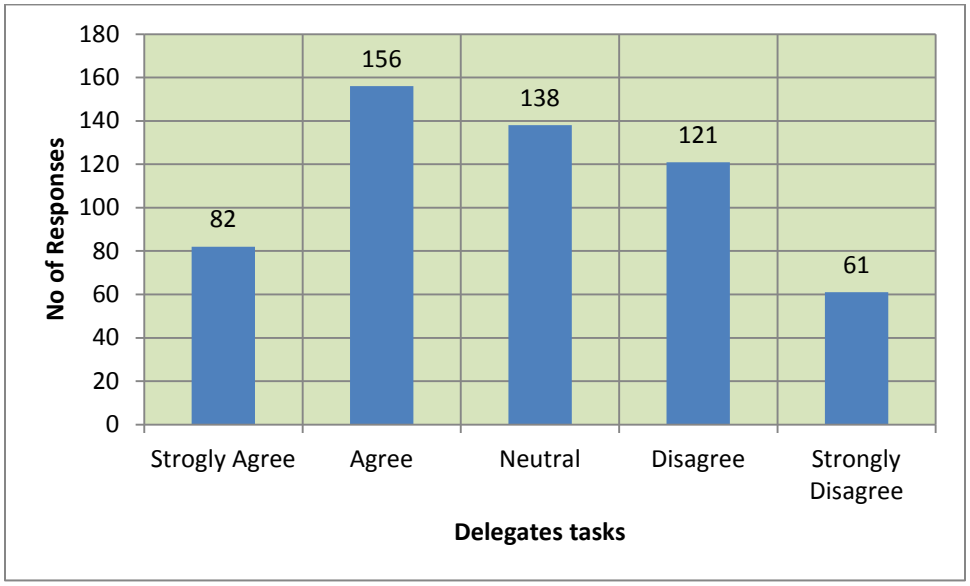

Figure 4-7: Implementing a new procedure or process.

Figure 4.8 shows the responses to the following statement: 'Hospital leadership likes to share information security power with employees'. The vast majority, 337 out of 588, strongly agreed or agreed with the statement, and only 146 out of 558 strongly disagreed or disagreed.

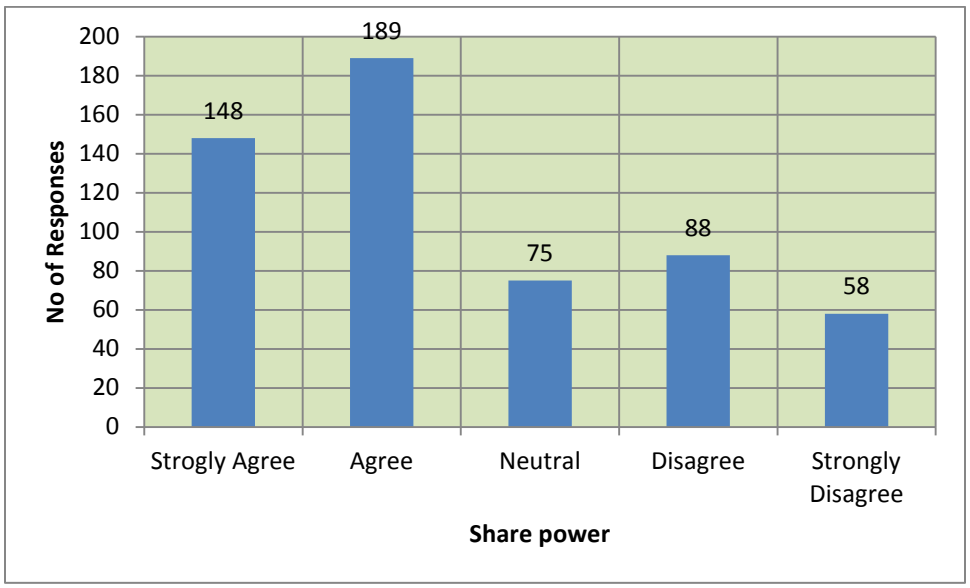

Figure 4-8: Hospital leadership likes to share IS power with employees.

Figure 4.9 shows the responses to the following statement: 'Hospital takes group vote on what to do next regarding the hospital information security policy'. The vast majority, 308 out of 588, strongly agreed or agreed with the statement, and only 161 out of 558 strongly disagreed or disagreed.

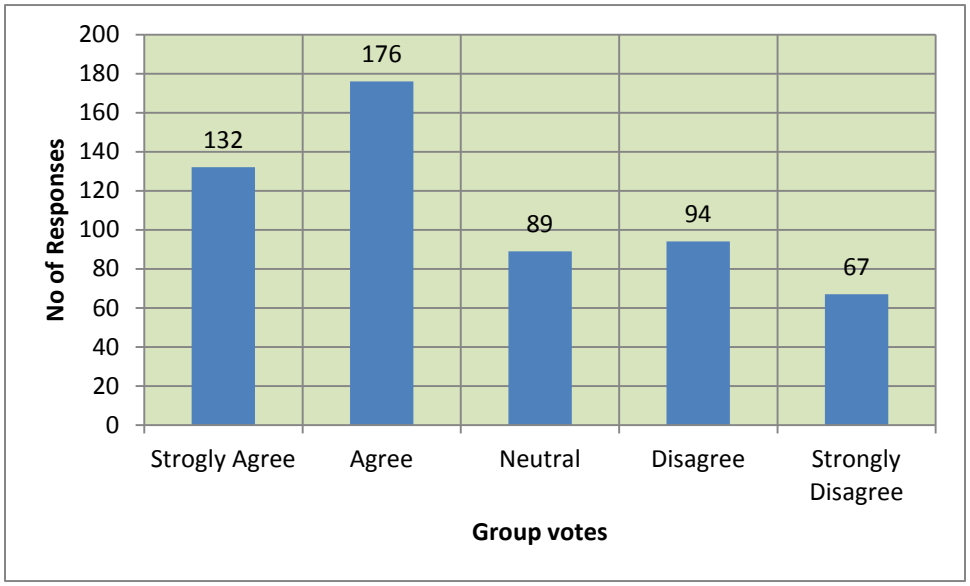

Figure 4-9: Hospital takes group vote on what to do next in the IS policy.

Figure 4.10 shows the responses to the following statement: 'National culture has influenced the leadership style in the hospital information security culture'. The vast majority, 444 out of 588, strongly agreed or agreed with the statement, and only 82 out of 558 strongly disagreed or disagreed.

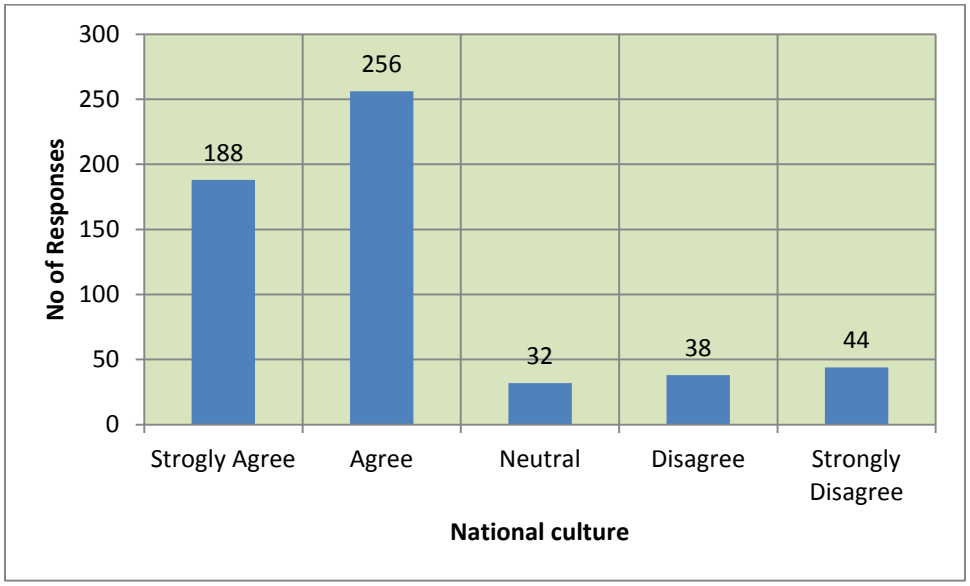

Figure 4-10: National culture has influenced the leadership style in the hospital IS culture.

Figure 4.11 shows the responses to the following statement: 'National culture values and norms have a role in the leadership information security decision-making processes. The vast majority, 372 out of 588, strongly agreed or agreed with the statement, and only 138 out of 558 strongly disagreed or disagreed.

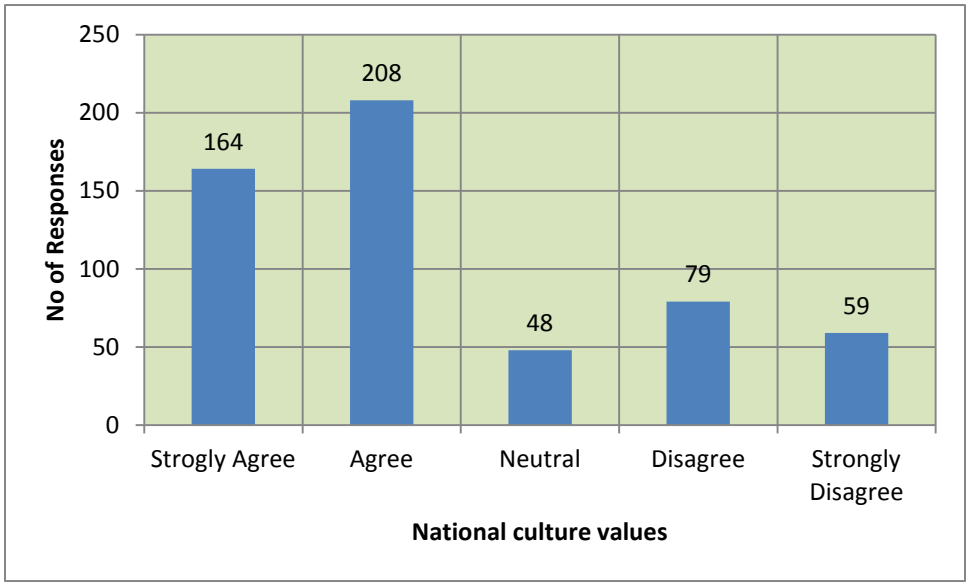

Figure 4-11: National culture values and norms have a role in the leadership IS decision-making process.

4.4 Hospital Culture

Figure 4.11 shows the responses to the following statement: 'Change in the hospital information security policy from traditional to electronic is a challenge'. The vast majority, 321 out of 588, strongly agreed or agreed with the statement, and only 159 out of 558 strongly disagreed or disagreed.

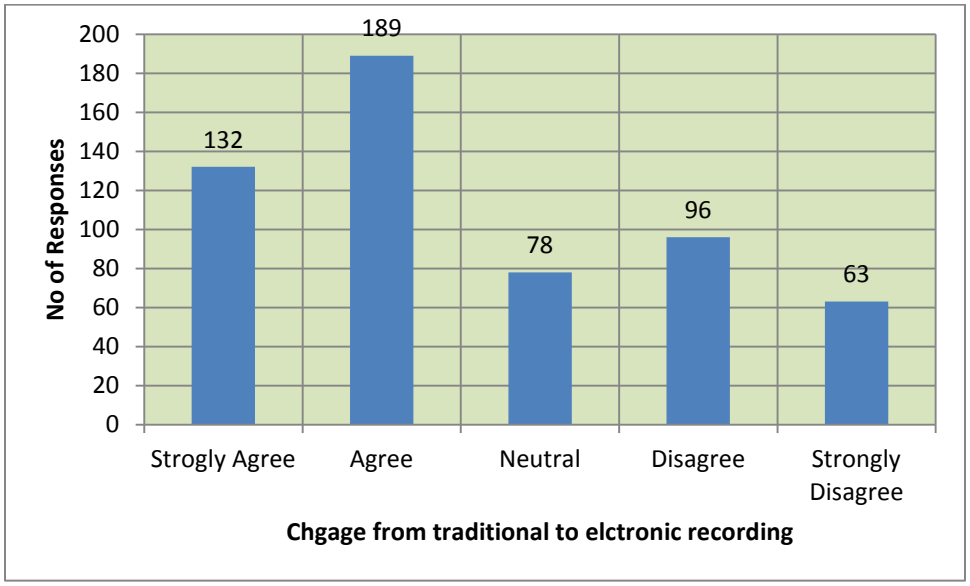

Figure 4-12: Change in the hospital IS policy from traditional to electronic is a challenge.

Figure 4.13 shows the responses to the following statement: 'The hospital uses an effective information security policy to protect electronic patient records'. The vast majority, 332 out of 588, strongly disagreed or disagreed with the statement, and only 134 out of 558 strongly agreed or agreed.

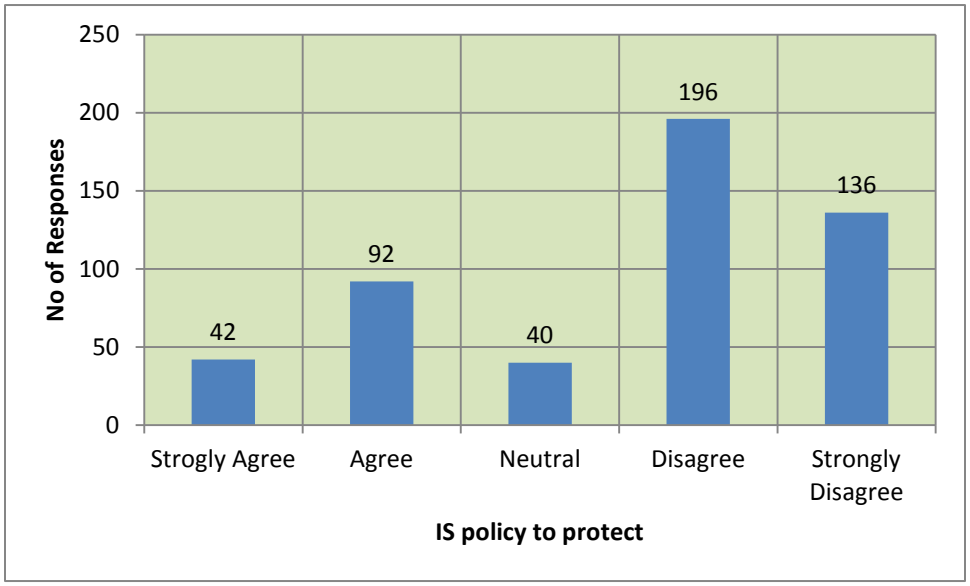

Figure 4-13: The hospital uses an effective IS policy to protect EPR.

Figure 4.14 shows the responses to the following statement: 'Hospital employees have positive norms and values towards information security'. The vast majority, 331 out of 588, strongly disagreed or disagreed with the statement, and only 151 out of 558 strongly agreed or agreed.

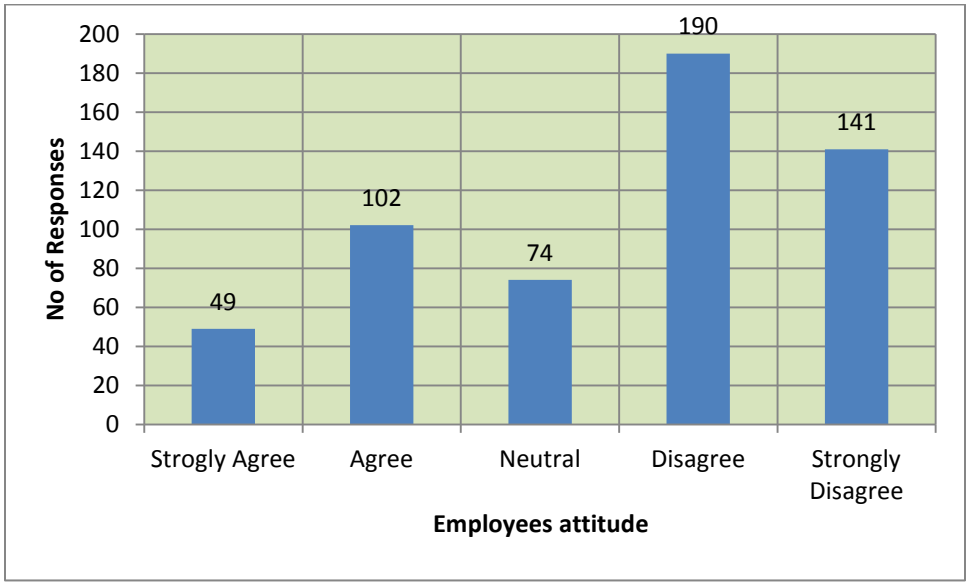

Figure 4-14: Hospital employees have positive norms and values towards information security

Figure 4.15 shows the responses to the following statement: 'The hospital has an appropriate information security environment'. The vast majority, 368 out of 588, strongly disagreed or disagreed with the statement, and only 121 out of 558 strongly agreed or agreed.

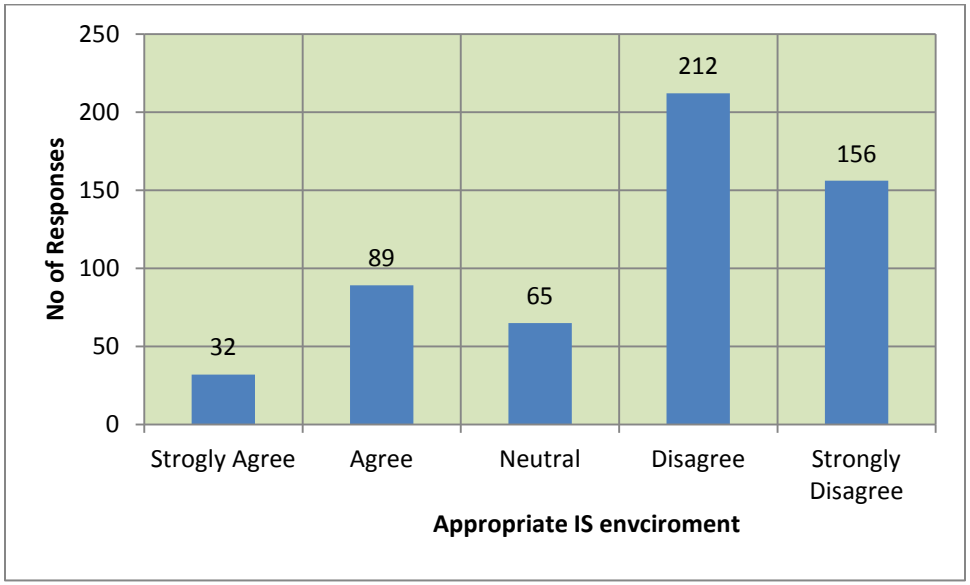

Figure 4-15: The hospital has an appropriate information security environment.

Figure 4.16 shows the responses to the following statement: 'Trust among the hospital employees is important for hospital information security'. The vast majority, 328 out of 588, strongly agreed or agreed with the statement, and only 161 out of 558 strongly disagreed or disagreed.

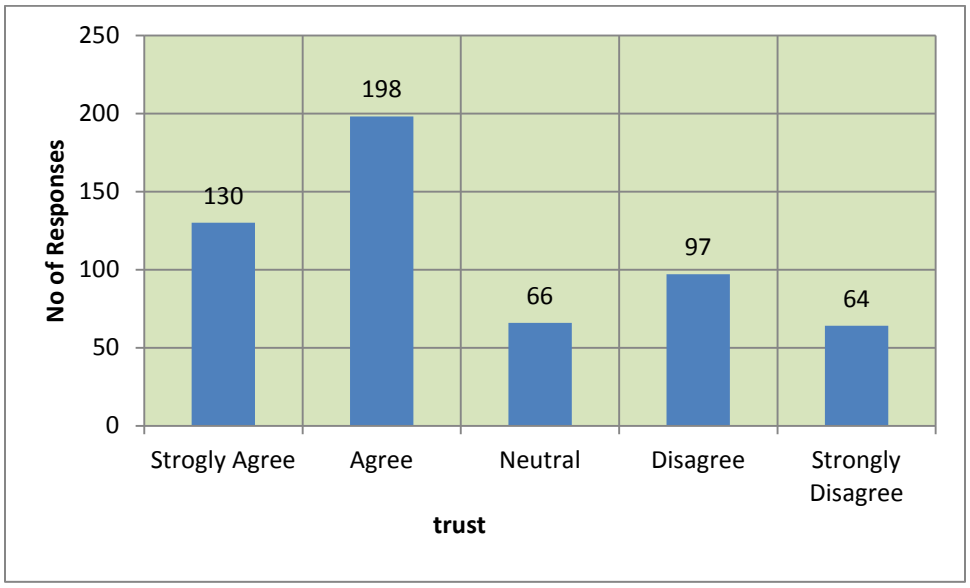

Figure 4-16: Trust among the hospital employees is important for the hospital information security.

Figure 4.17 shows the responses to the following statement: 'There is a lack of trust amongst the employees due to a lack of an effective hospital culture'. The vast majority, 302 out of 588, strongly disagreed or disagreed with the statement, and only 173 out of 558 strongly agreed or agreed.

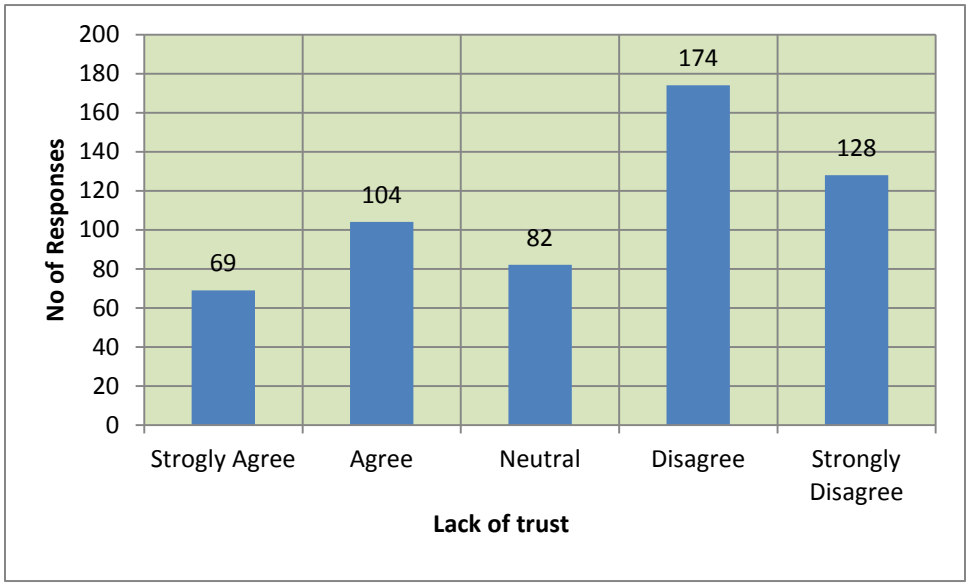

Figure 4-17: Lack of trust amongst the employees due to lack of effective hospital culture.

Figure 4.18 shows the responses to the following statement: 'Trust between the employees and management is important for information security'. The vast majority, 311 out of 588, strongly disagreed or disagreed with the statement, and only 148 out of 558 strongly agreed or agreed. The main drive for the disagreement with the statement due to lack of awareness of the employees.

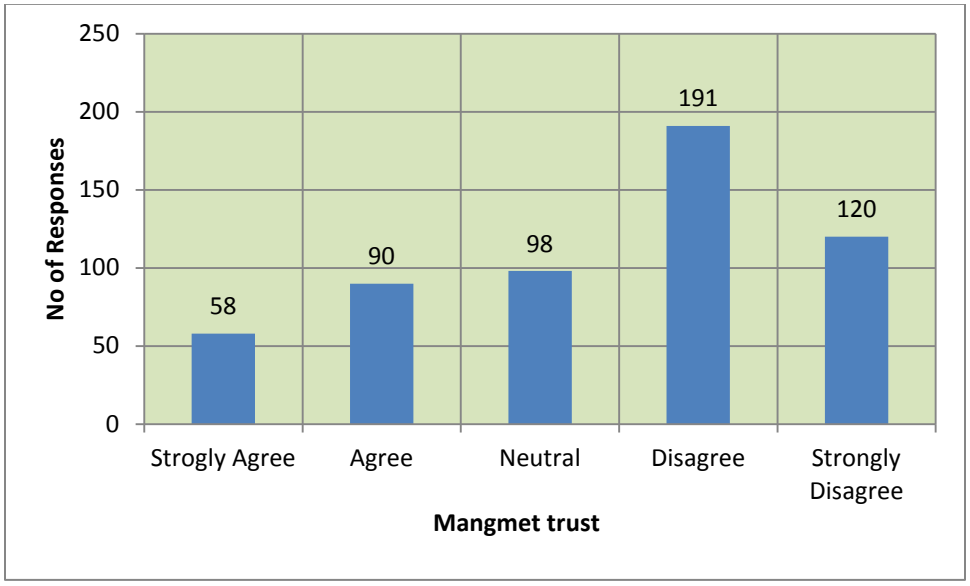

Figure 4-18: Trust between the employees and management is important for IS.

Figure 4.19 shows the responses to the following statement: 'There is a lack of trust between the employees and technology regarding information security'. The vast majority, 328 out of 588, strongly agreed or agreed with the statement, and only 185 out of 558 strongly agreed or agreed.

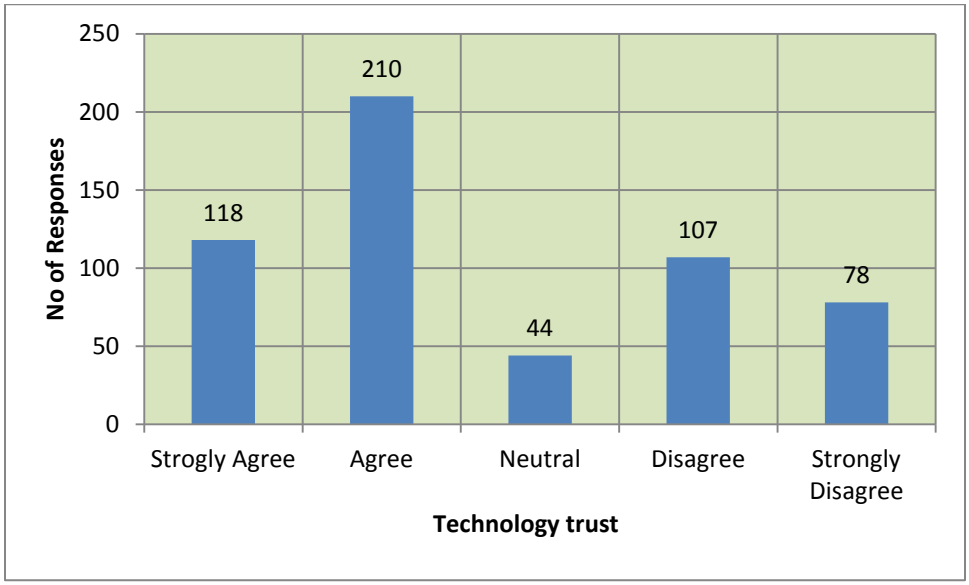

Figure 4-19: There is a lack of trust between the employees and technology regarding IS.

Figure 4.20 shows the responses to the following statement: 'A shift from traditional medical recording to electronic recording represents a threat to job security'. The vast majority, 251 out of 588, strongly agreed or agreed with the statement, and only 202 out of 558 strongly disagreed or disagreed.

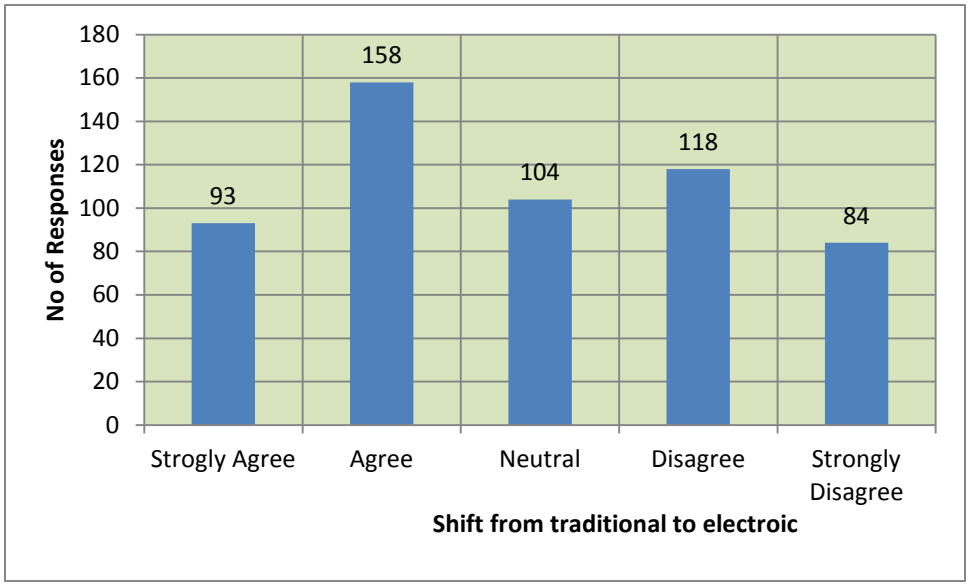

Figure 4-20: Shift from traditional to electronic recording represents a threat to job security.

4.5 Hospital Information Security Policy Culture

Figure 4.21 shows the responses to the following statement: 'Hospital has a clear information security policy'. The vast majority, 416 out of 588, strongly disagreed or disagreed with the statement, and only 108 out of 558 strongly agreed or agreed.

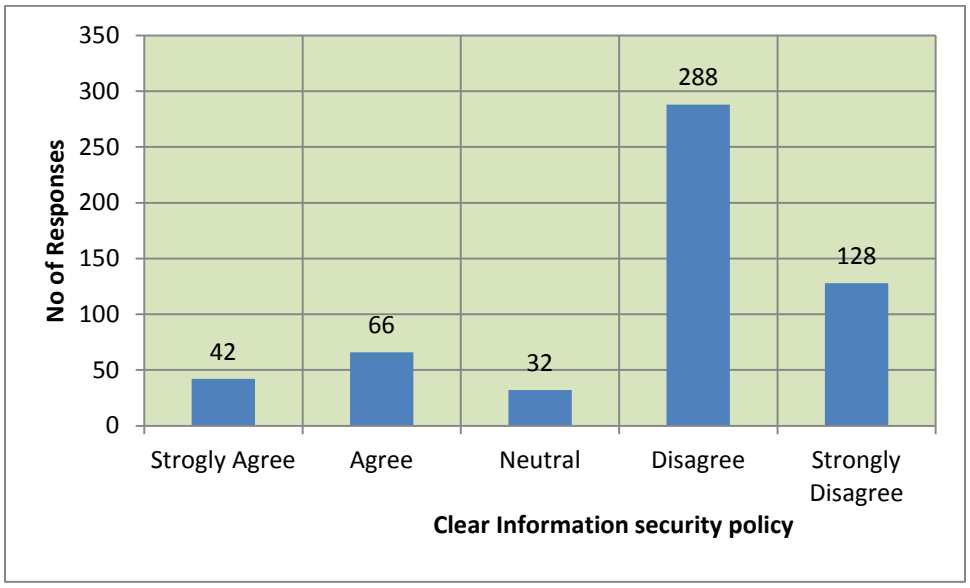

Figure 4-21: Hospital has a clear information security policy.

Figure 4.22 shows the responses to the following statement: 'Hospital employees are aware of the current information security policy'. The vast majority, 319 out of 588, strongly disagreed or disagreed with the statement, and only 165 out of 558 strongly agreed or agreed.

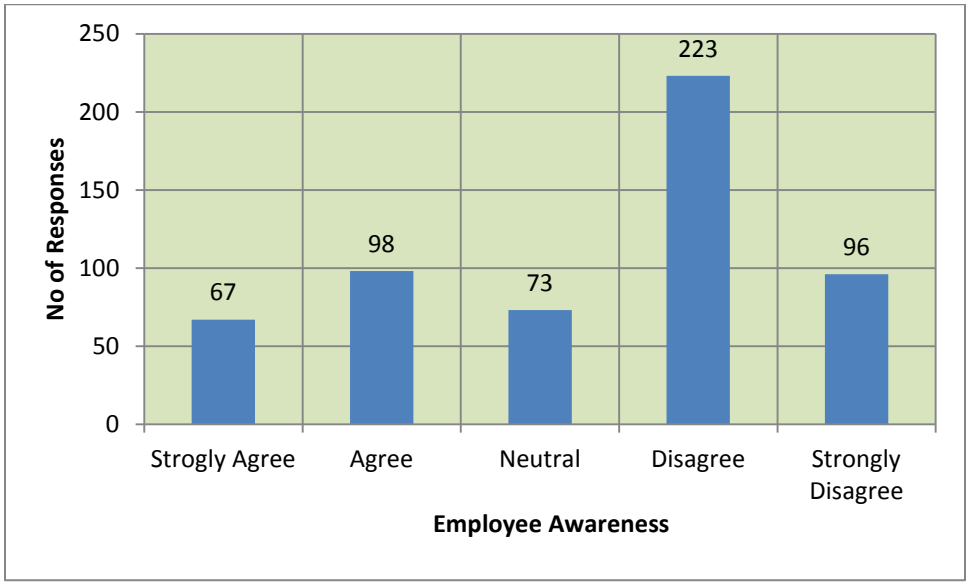

Figure 4-22: Hospital employees are aware of the current information security policy.

Figure 4.23 shows the responses to the following statement: 'Hospital employees are aware of the importance of health information security'. The vast majority, 253 out of 588, strongly disagreed or disagreed with the statement, and only 215 out of 558 strongly agreed or agreed.

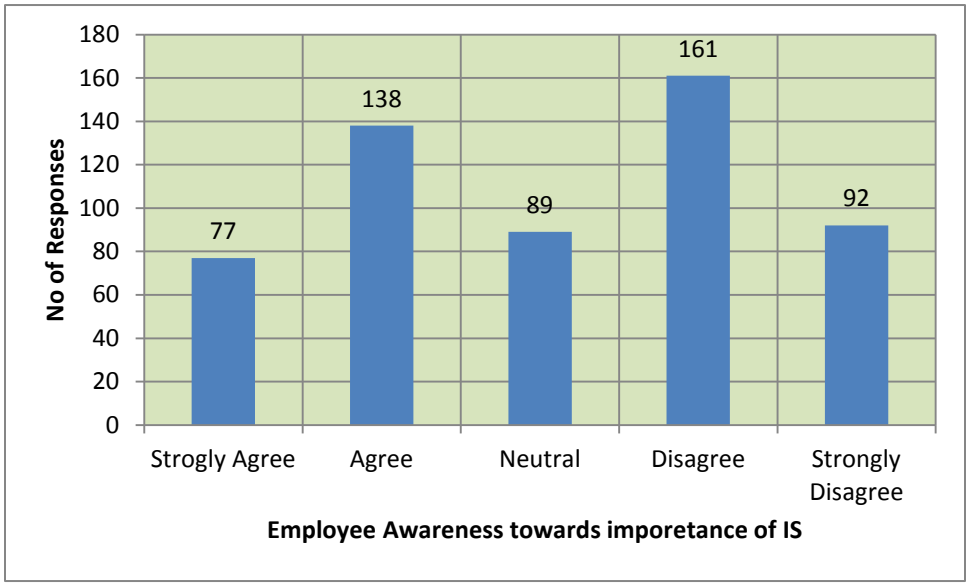

Figure 4-23: Hospital employees are aware of the importance of health IS.

Figure 4.24 shows the responses following the employees' training in information security. The vast majority, 372 out of 588, strongly agreed or agreed with the statement, and only 139 out of 558 strongly disagreed or disagreed. And 49 out of 588 stayed neutral.

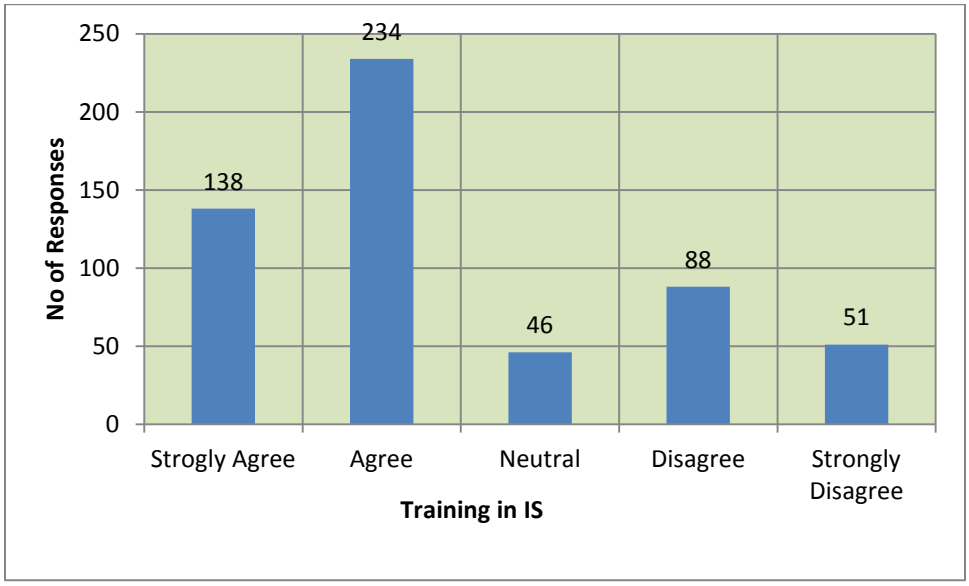

Figure 4-24: The employees have never been on a training course regarding IS.

Figure 4.25 shows the responses to the following statement: 'Employees do not respect the current information security'. The vast majority, 325 out of 588, strongly agreed or agreed with the statement, and only 163 out of 558 strongly disagreed or disagreed, and 64 out of 588 neutral.

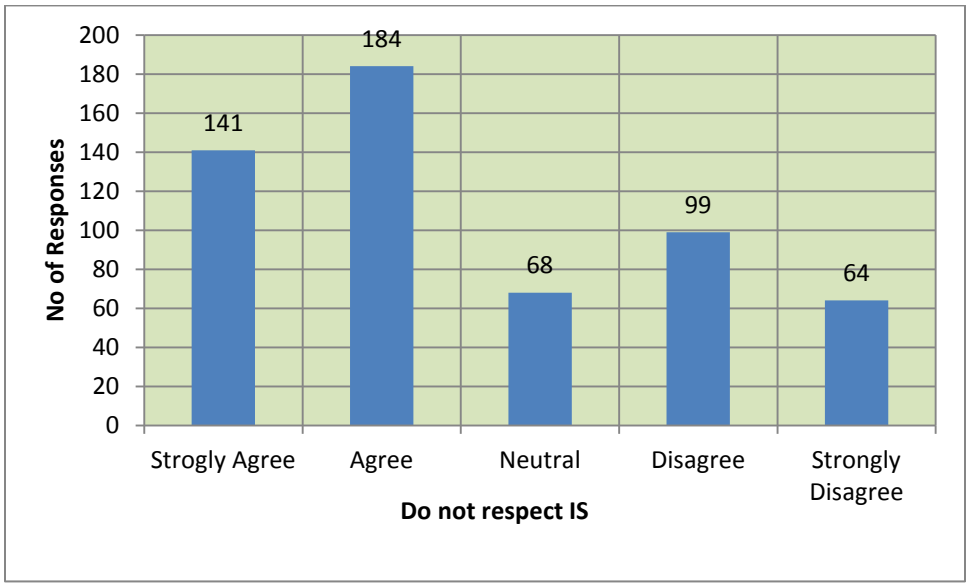

Figure 4-25: Employees do not respect the current information security.

Figure 4.26 shows the responses to the following statement: 'the current IS does not reflect the current use of electronic recording'. The vast majority, 388 out of 558, strongly agreed or agreed with the statement, and only 144 out of 558 strongly disagreed or disagreed and only 24 of the respondents preferred to stay neutral.

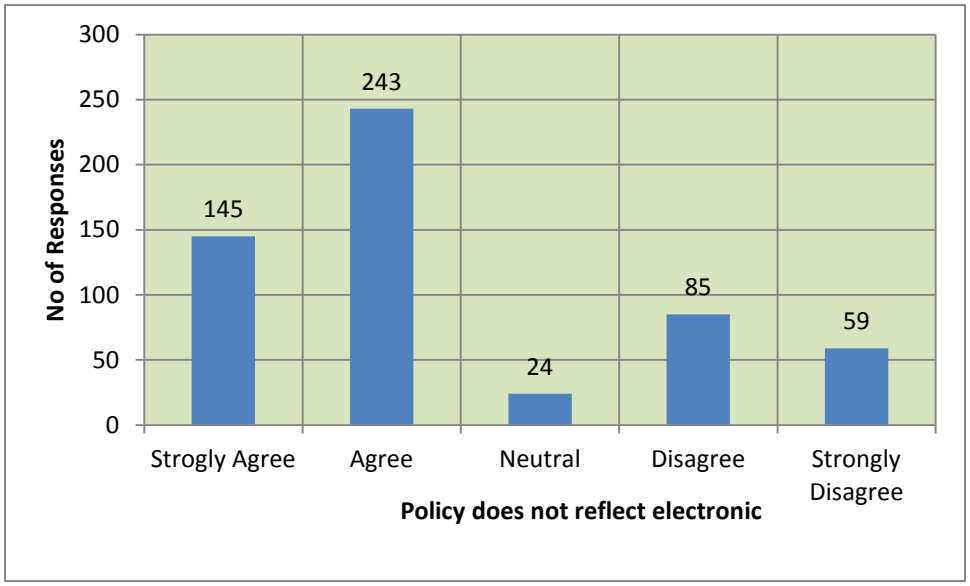

Figure 4-26: The current IS does not reflect the current use of electronic recording

Figure 4.27 shows the responses to the following statement: 'The current policy does not take patients' rights into consideration '. The vast majority, 435 out of 588, strongly agreed or agreed with the statement, and only 104 out of 558 strongly agreed or agreed with only 28 out of the 588 neutral.

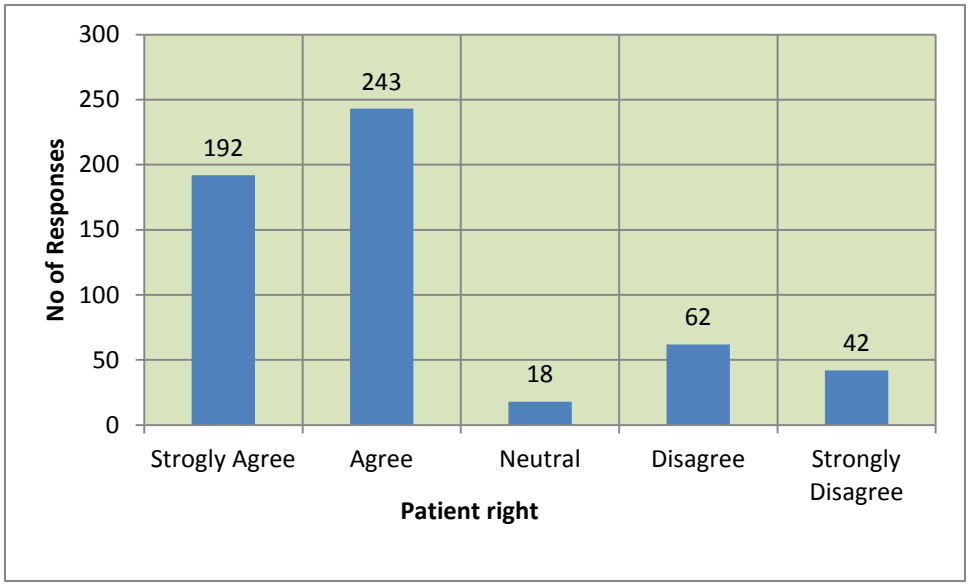

Figure 4-27: The current policy does not take patients' rights into consideration

4.6 Role of National Culture on Information Security

Information security behaviour within health services is possibly influenced by an individual's national culture. Figure 4.28 shows the responses to the following statement: 'Individual behaviour within an organisation may be influenced by an individual's national culture, values and norms'. The vast majority of the responses, 61.8% (345 out of 558), strongly agreed or agreed with the statement, and only 22.2% (124 out of 558) strongly disagreed or disagreed, while 15.9% (89 out of 558) remained neutral.

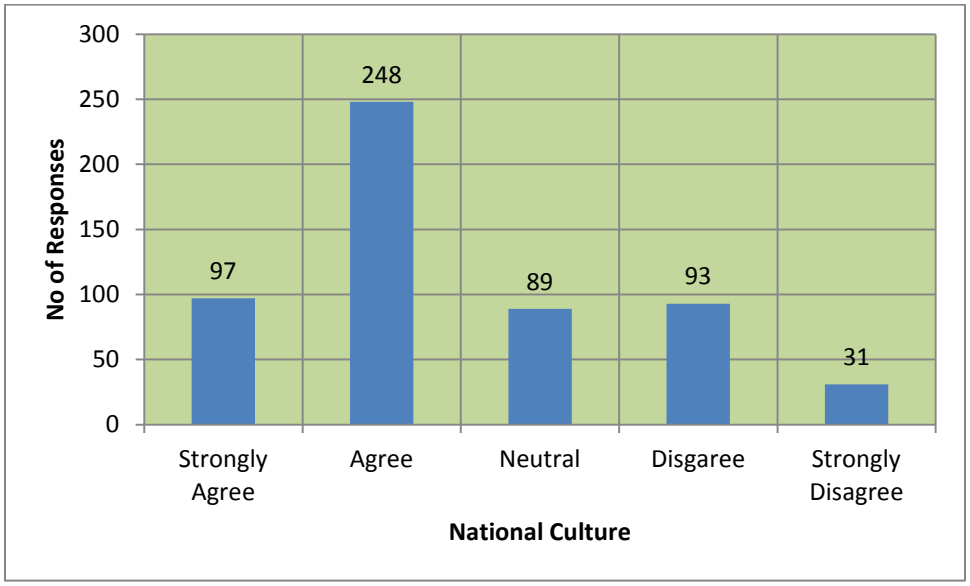

Figure 4-28: Employees' behaviours are influenced by national culture

One of the cultural sub-dimensions that are most interesting in this research is the role and impact of the Saudi national culture on information security culture. One of the statements presented to the SA health service employees was that the Saudi national culture has influenced the hospital information security culture. The vast majority of the responses, strongly agreed or agreed with the statement, and a minority strongly disagreed or disagreed.

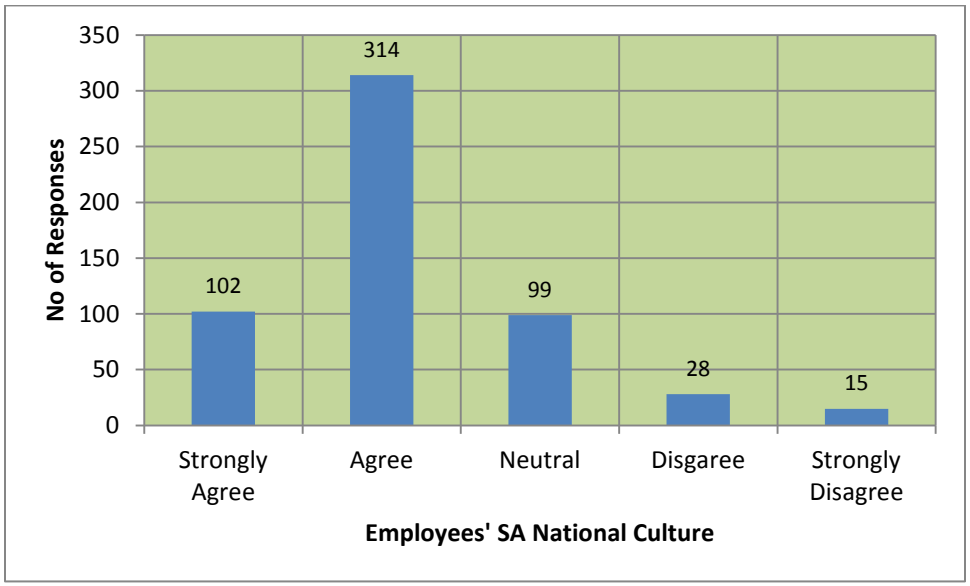

Figure 4-29: SA national culture influences information security culture.

The SA BHS has a large number of non-nationals working for the services. This is mainly due to the lack of skills and competence present in employees in the health service sector. This has created several sub-cultural groups within the field of health service. These groups have their own values and norms. For example, there is a large number of nurses from Philippines and Asia as well as a large number from Egypt on the medical staff. Therefore, it is important to analyse whether such sub-cultural groups within the hospital's working environment have

impacts on the information security culture. The SA health service employees expressed their opinions towards the statement reflecting the impact that the social division of the groups within the hospital has on the hospital information security culture. The majority of the responses, (227 out of 557), 41% strongly disagreed or disagreed with the statement, and (212 out of 557) 38% strongly agreed or agreed, and (118 out of 557) 21% remained neutral.

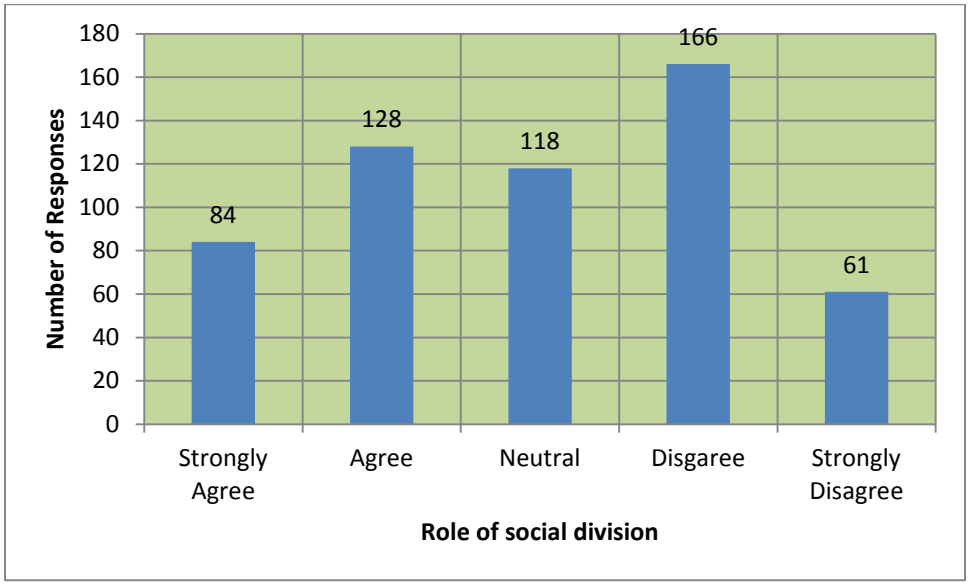

Figure 4-30: Role of social division on hospital IS culture

Although Arabic is the official language used in the hospitals, there are other languages used in the hospital working environment. This includes English, which is used by Western expatriates. Different languages used in the hospital are barriers for the hospital information security culture. This has influenced understanding and communication processes among the hospital employees. Therefore, it is important to identify the employees' opinions towards the role of using different languages in the hospital working environment on the information security

culture. The majority of the responses, (295 out of 557) 53% strongly disagreed or disagreed with the statement, and (194 out of 558), 35% strongly agreed or agreed, while (69 out of 558), 12% remained neutral.

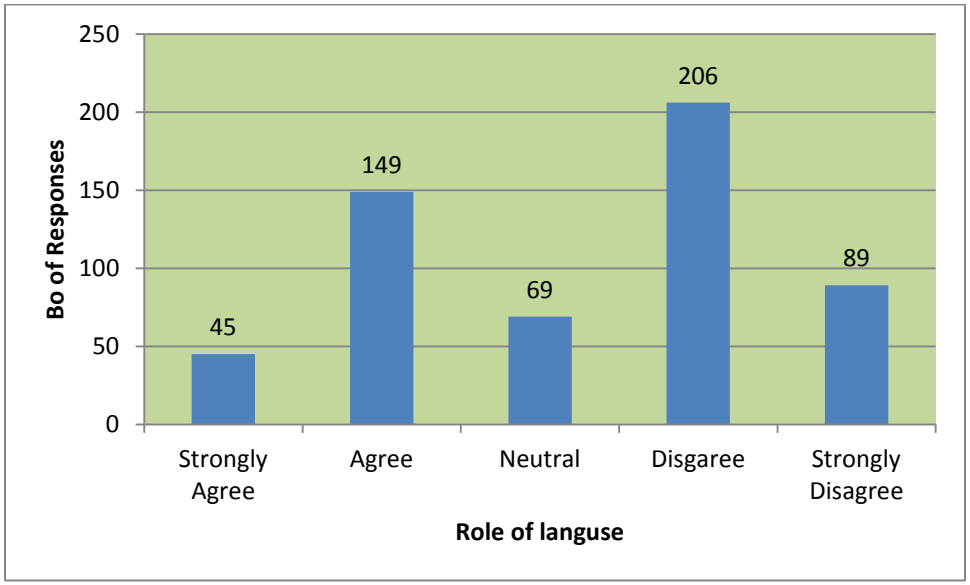

Figure 4-31: Role of languages used on IS culture

The hospital management is responsible for creating a positive information security culture within their hospitals. The vast majority of the hospital management staff members are Saudi nationals with distinctive conservative SA national culture. The survey is aimed at identifying the hospitals' opinions towards the following statement: 'Saudi national culture has influenced the hospital management information security policy'. The majority of the responses, (355 out of 558), 64% strongly agreed or agreed with the statement, and (154 out of 558) 28% strongly disagreed or disagreed, while (49 out of 558) 8% remained neutral.

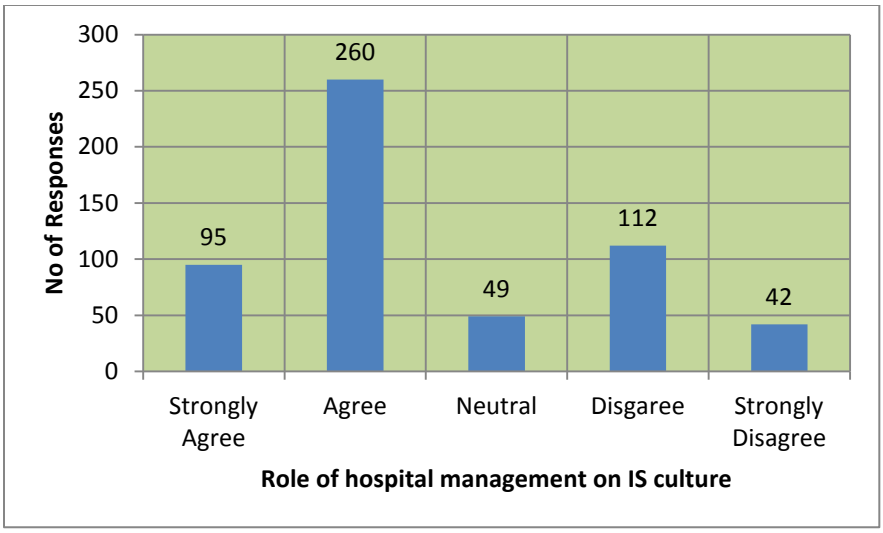

Figure 4-32: Role of SA hospital management on IS culture

Social interaction of the employees can be argued to be an effective tool in building employees' trust, respect and understanding of each other. Social interaction within the hospital's working environment helps build understanding and trust among employees. This helps in developing positive hospital information security culture. The majority of the responses, (238 out of 558), 43% strongly agreed or agreed with the statement, and (226 out of 558) 40% strongly disagreed or disagreed, while (94 out of 558) 17% remained neutral.

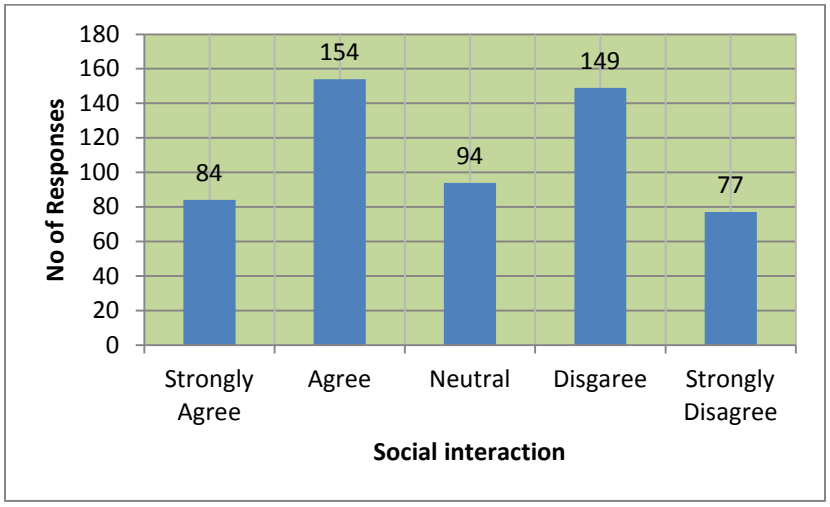

Figure 4-33: Employees' social interaction has helped to improve IS

4.7 Summary

The researchers analysed the quantitative data of the chapter to identify the main cultural dimensions. The analysis is based on distributing semi-structured questionnaires to key personnel at Saudi National Health Service hospitals. This is needed to identify the information security cultural dimensions that influence individual employees' behaviour towards information security within the hospital working environment.

The next chapter, Chapter 5, presents qualitative data to enhance the quantitative data analysis of this chapter and explore any cultural dimensions that the author is not aware of. The outcomes of this chapter and the next chapter will be used to develop the information security cultural model.

CHAPTER 5
DATA ANALYSIS: QUALITATIVE DATA ANALYSIS

Chapter 5 Objectives

The main objectives of this chapter are as follows:

- Interviewing key personnel in SA health services;
- Discussing hospitals' employees perceptions and attitudes towards information security;
- Exploring and identifying information security culture dimensions and sub-dimensions;
- Exploring and discussing the current information security culture policy and changes needed.

Chapter 5 Data Analysis: Qualitative Data Analysis

5.1 Introduction

The analysis identified the main culture-related dimensions that have a role and impact on a hospital's information security culture. The quantitative data analysis needs enhancing and clarification, as well as the inclusion of in-depth information regarding the culture-related dimensions. Additionally, a qualitative data analysis is needed to help understand the main factors of the current information security culture and to provide in-depth information for the culture-related factors.

This chapter presents an analysis of the one-to-one interviews with 15 key employees from three main national hospitals in Saudi Arabia. The interviewees were selected based on their experience and job description (their role in the patient care process). The interviews were carried out at the hospitals by appointments as convenient for the interviewees. The main outcomes of the qualitative data were combined with the main outcomes of the quantitative data to develop the research culture-related model, which is illustrated in Chapter 6. An interview analysis is needed to explore and discuss the culture-related dimensions based on the interviewees' attitudes, experiences and understandings of the current information security culture at their respective hospitals. This type of information is difficult to explore and is discussed in the quantitative data analysis. The main aim of the interviews is to explore the information security culture dimensions in order to use them in developing an effective information security culture.

Table 5.1: Interview participants

No	Hospital	Job and Expertise	Notes
1	Consultant	Hospital A	Senior medical staff that makes decisions on patients records
2		Hospital B	
3		Hospital C	
4	Hospital Manager	Hospital A	Manage physical and human resources of the hospital
5		Hospital B	
6		Hospital C	
7	Medical Doctor (Physician)	Hospital A	Direct interactions with patients and are involved in updating patient's medical records
8		Hospital B	
9		Hospital C	
10	Nurse	Hospital A	Direct carer through the patient health care process
11		Hospital B	
12		Hospital C	
13	Administrator	Hospital A	Involved in the patient healthcare process from the administration's point of view
14		Hospital B	
15		Hospital C	

5.2 Employee and Information Security

Hospital employees are the main factors influencing hospital culture. The employees' roles and impacts, from a human point of view, are the main focus of the research. The role of employees in the hospital security culture was explored and discussed in all of the interviews. The interviewees in the three hospitals agreed and stressed those employees' behaviours and attitudes towards information security are the main threats to information security. One of the interviewees affirmed this statement directly in the following:

> 'I think one of the main threats to information security is the employees' behaviour and attitudes towards information security'
>
> (Interviewee B).

One of the issues explored in the interviews that had an impact on information security is employee job dissatisfaction. The interviewees argued that job satisfaction plays an important role in employees' behaviour, attitudes towards information security, interactions with health service users and interactions with other hospital employees. The interviewees stated that due to a lack of job opportunities in the Saudi market, hospitals have employed a large number of people in health care administration jobs without appropriately assessing the individuals' motivation or commitment to working in the hospitals. This has led to the employment of employees without the right attitudes or proper commitment to information security in the hospital culture.

One of the hospital's employees breached a patient's information security. As a result, it is evident that there are several employees working in the hospitals without the right motivation and commitment. This job dissatisfaction has an impact on the employees' commitment towards medical information security.

The interviewees stated on several occasions that the employees' attitudes, awareness, and commitment towards hospital information security can be classified into two main categories. The first group is highly committed and aware of the importance of keeping the patient's medical information confidential. This group mainly consists of highly qualified medical staff, such as consultants and specialists. The second group is less aware of or committed to maintaining information security. This group consists of non-medical staff members, especially administrators and medical technicians. This also reflects the diversity and complexity of the hospital's culture. Regarding this issue, one of the interviewees stated the following:

> 'I can confidently say that, in the hospital, [there are] different attitudes and commitments toward medical information. There is a group [that is] quite aware [of], understands, [and is] committed towards medical information'
>
> (Interviewee B).

The other important issue explored in the interviews involved the patient's rights towards his or her medical records. The interviews also explored the right to ownership of the medical record. The interviews indicated diversity in the interviewees' opinions towards patients' rights and ownership of their medical records. However, the typical norms and traditions that were shown by the employees' daily interactions is that the hospital owns the medical records and has little understanding and awareness of the patient's rights. The culture indicates that medical information is transferred and discussed without the patient's consent. The interviewees also indicated that there is no clear patient consent form, clear policy, or clear processes for transferring patients' medical records between health organisations or with other institutions, such as policy or insurance companies. Some of

the interviewees stated that the security and confidentiality of the patient's medical information is the patient's right:

> 'Patient medical information security is the patient's right. There is a need to understand this right and establish appropriate and clear policy in this regard'
>
> (Interviewee B).

The attitudes and awareness of the employees has been reflected in the employees' behaviour within the hospital culture. It has become the norm to pass patients' medical information on to a third party when deemed appropriate. Unfortunately, in some cases, employees valued passing medical information and believed it to be their social responsibility and commitment. This attitude and behaviour represents one of the main problems of hospital information security. One of the cases regarding administrators' attitudes is explored by one of the interviewees:

> 'One day, I challenged the hospital administrator [who was] passing patent medical information to an external user. He replied, with confidence, [that] this is part of social and professional responsibility. I replied, "Social responsibility without patient consent"' (Interviewee B).

One of the main challenges for the health authority members in Saudi Arabia is the need to invest more in human resources. There is a feeling amongst hospital employees that the health service authority has not invested in medical and non-medical staff. From an information security point of view, employees' awareness, education and knowledge are critical to ensure information security in a hospital. Therefore, investing in employees through training is an important component of promoting a positive information security culture. The authority is investing in medical physical resources and medical staff before the employee. Put simply, the

authority needs to invest more in employee education, such as information security (Interviewee B).

5.3 Leadership and Information Security Culture

One cultural factor is the role of hospital leadership on the hospital's information security culture. The interviews explored several factors that influenced the development of the hospital leadership's views. Individual cultures, such as Saudi culture, have influenced the leadership style of the hospital culture. One of the main factors explored in the interviews is that the current hospitals' leadership lacks a clear vision in information security culture:

> 'I would say confidently that the hospital lacks clear vision towards information security culture'
> (Interviewee E).

The interviews also explored the idea that hospital leadership has an important role in promoting and enhancing employees' trust. Leadership has a role in establishing an appropriate environment, motivating the employees, and encouraging formal and informal interactions among the employees. Arguably, these factors play an important role in promoting and enhancing trust among the employees. One of the interviewees addressed this issue in the following statement:

> 'In my opinion, the hospital leadership has a critical role in enhancing and promoting hospital staff trust, which is critical in information security'
> (Interviewee G).

The research explored the role and impact of technology on employees' trust. Discussions with several employees led to the conclusion that modern technology plays an important role in facilitating interactions amongst the employees, as well as facilitating knowledge sharing, social interaction and help in understanding. This is mainly due to the role of technology in enhancing understanding and respect amongst the employees through the use of the technology. Understanding and respect between employees helps to promote trust among the employees of the hospitals. One of the interviewees explored this issue by stating that

> 'the modern technology creates an excellent tool for hospital employees' interaction and helps in creating and developing trust among the employees'
>
> (Interviewee C).

Technology, can be an excellent tool for promoting a culture that values information security. Several interviewees explored technology as a tool for training and promoting an information security policy, as well as for promoting information security education tools. They stressed the use of technology, such as the use of three-dimensional visual information security scenarios and case studies online, for employee training and education. One of the interviewees stressed this issue strongly by stating the following:

> 'I trust…technology needs to be used in training and promoting information security awareness, education, and daily behaviour. Use of technology in promoting three-dimensional visual scenarios in other industries can be adopted and used in the hospital's information security awareness and education' (Interviewee F).

From the point of view of promoting Saudi information security, the authority needs to invest in technology to promote and enhance a culture that values information security. This is necessary because of the complexity of Saudi national culture and its attitudes towards

information security. The health service authority needs to take advantage of developments in technology, such as in hardware and software, as well as taking influence from developing countries' health information security to promote and enhance the Saudi health service's information security. These developments can be used in training, online training, seminars, case studies, scenarios and references to information security policy.

5.4 Role of Hospital Management on Hospital Culture

This section presents an analysis of the role and impact of hospital management on hospital information security. It is important to stress that the Saudi National Health Service is a public service; there are limited private hospitals in the Kingdom. The role of the service includes managing the hospital budget, recruiting medical; and non-medical staff, strategic planning and enforcing policies.

5.4.1 Medical Staff vs. Management Staff

An important dimension considers the cultural differences that arise in managing the hospital. The first opinion is held by the hospital senior medical staff, such as consultants. Senior medical staff members believe that senior medical staff should manage the hospital. They believe that the senior medical staff members are more aware, that they understand the hospital processes and operations and that they better understand the medical staff's needs and feelings. On the other hand, the non-medical senior staff members believe that the hospital should be managed by non-medical staff, which would leave the senior medical staff to concentrate on patients' medical care. They believe that the hospital organisation needs to be managed as though it is a business, which should be led by non-medical staff. This

difference has created an uncomfortable situation in the hospitals, as senior medical staff found it difficult to accept the decisions and strategies developed and implemented by non-medical staff. One of the senior medical staff explored this issue and stated the following:

> 'In my view, the hospital should be managed by senior medical staff because they understand the profession better, understand the profession's needs, and, most importantly, they have the future vision and expectation of the future health service's needs'
> (Interviewee E).

Non-medical staff in managerial posts argued strongly that health services and hospitals need to be managed by non-medical staff. They argued that health services and hospitals have become enterprises, and there is a need for skilled, experienced, and competent individuals to manage these services. They argued that managers need to come from a business and management background, rather than from a medical background. The argument is based on the notion that senior medical staff need to be focused on providing and contributing to patients' medical services. Investment in medical staff is aimed at developing medical staff, not managers, and the only way to repay the government's investment in medical staff is by allowing them to focus on providing medical services to patients. The non-medical staff members at senior levels are aware of this. They admit there is a conflict of opinions and attitudes towards managing the health service. They are aware that medical staffs, especially senior medical staff, want to manage the health services that they provide. From the organisation's point of view, the culture is so divided that the health service need to be managed by a trusted team to eliminate division. This may create a conflict of interest, as well as conflicts in the implementation of instructions from the management to the employees, the flow of information and instructions throughout the health service. The most important division in opinions and attitudes

between the health service's management and working staff members at the organisation can lead to trust and respect between them, through interaction that promote awareness and understanding between them. This will have an impact on the organisation's performance such as on information security policy implementation and daily operational activities.

> 'I think and strongly believe the hospitals need good managers, not good physicians. Highly competent physicians are not necessary [to] be a good hospital manager, as a managerial post needs different skills and competences. Unfortunately, within the hospital and within the Kingdom Health Services Authority, there is an attitude and belief that hospitals should be managed and administrated by the senior medical staff. In my view, this [is] a wrong attitude [and]…wrong view and needs to be changed'
>
> (Interviewee F).

The interactions and communication amongst medical staff, especially at the senior level and amongst management, were explored as one of the culturally based problems. Medical staff members were found to be uncomfortable taking instruction from management personnel without medical backgrounds. This has clearly created clashes and a lack of trust between the groups. This problem was made clear when one interviewee stressed that their management introduced medical staff scheduling and ordered physical resources without the active involvement of senior medical staff. Such a problem develops a culture of conflict between medical staff members and the management. From an information security point of view, such a conflict will have an impact on information security. This impact can be seen in two ways. The first impact is in the implementation of the information security policy by the medical staff through the management's instructions. This will be an issue due to the fact that there will be a lack of trust and belief in the management teams by medical staff. The second impact is in the flow of

information from the management team to the medical staff. These two impacts will contribute to the information security culture of the hospital. This issue was clearly emphasised by one of interviewee when he stated the following:

> 'Of course, based on my personal experience in the hospital, medical staff, especially senior medical staff, [when] getting instruction from non-medical staff managers, [are] uncomfortable, due to a lack of trust and belief in medical staff or the hospital management' (Interviewee B).

5.4.2 Management Commitment

Management's commitment towards developing a positive information security culture is critical. Due to the structure of the Saudi National Health Service, the public sector and the management are the main decision makers in all of the health service's operations and strategies, including the information security culture policy, implementation, promotion and investment in information security culture.

Management commitment towards the information security culture was explored and discussed by several interviewees. They indicated that management commitment is critical in creating an appropriate hospital information security culture and protecting the integrity and confidentiality of patients' medical records. The interviewees indicated that the hospitals' management lacks the appropriate commitment to promoting and enhancing the hospital information security policy. This lack of commitment was, arguably, because of a lack of understanding and awareness of the role and impact of hospital culture on information security. In this regard, one of the interviewees stated the following:

> ‘I can say with confidence that the management lacks commitment towards enhancing and ensuring medical information security and, especially, the patient medical records, such as the electronic medical staff’
>
> (Interviewee C).

The main explanation for the lack of management commitment to the hospital’s information security culture is the hospital management’s priorities. One of the interviewees stated that the hospital management, at this stage, has several important priorities that may be ahead of the information security culture. It can be argued that the Saudi National Health Service is still in the process of developing and creating the most appropriate structure to improve hospital performance and efficiency. One of the interviewees explored this issue by stating the following:

> ‘We do care [about] and understand the importance of information security and, in particular, the security of the patient records. The main reason for not yet having a robust information security policy is [that] the management is still in the process of establishing the hospital activities and structures. I would say there are some priorities for the health service, alongside information security’
>
> (Interviewee F).

Other interviewees echoed the lack of management’s commitment towards promoting and enhancing the hospital’s information security culture. The interviewees stated in several statements that the hospital management has not shown any commitment to introducing information security culture strategies, policies and guidelines. They stressed that the hospital’s management also failed to invest in promoting and enhancing information security culture through developing appropriate training courses and establishing appropriate working environments to help develop an appropriate information security culture. One of the interviewees explored this issue by stating the following:

> ‘To be honest, I have not seen or observed any serious commitment or motive from the management to enforce or commitment to enhance the security of the medical information. I am stressing this from a practising point of view’ (Interviewee G).

The other important issues that were explored were the financial commitment from the Ministry of Health and hospital management. Financial commitment is needed in two main areas. The first is the need to invest in the human part of the hospital culture through training and establishing trust and understanding amongst employees. The second is to invest in developing and enhancing the hospital’s cultural environment. The interviewees stressed that there is no financial budget established by the Ministry of Health or hospital management to promote hospital culture and to develop an appropriate information security policy. One of the interviewees stated the following on this issue:

> ‘My understanding [is that] there is no financial commitment for promoting and enhancing information security culture. There is no budget [in] the hospital annual budget for information security culture, in general, and to information security culture, in particular’ (Interviewee G).

5.4.3 Information Security Policy

The hospital's information security policies mostly fall short in protecting patients' medical records. The current hospital policies are generic and antiquated. They concentrate on access control policy, which mainly use usernames and passwords to enter the hospital systems. The policy has been built mainly as a result of the abuse and misuse of passwords and usernames. There are no policies regarding the punishments and penalties for abusing the records or transferring information to a third party without permission and patient consent. One of the interviewees discussed this issue in the following statement:

> 'The hospital's main security policy is on [the] technical part, i.e., getting usernames and passwords to access medical information and not the human part of hospital activities' (Interviewee E).

The interviewees from the three surveyed hospitals agreed that their hospitals lacked any policy or strategy to promote and enhance their hospital's information security culture. Several interviewees explored this issue, and they stressed that there is a lack of consideration for the human role on the abuse and misuse of medical information. The hospital strategies, which reflect the Ministry of Health's strategy, fail to recognise hospital culture and the role of humans in abuse of hospital information security. One of the interviewees stressed this issue by stating:

> 'There is no policy or strategy to promote and enhance information security hospital culture in our hospital'
> (Interviewee G).

One of the other important issues explored in several interviews is that hospitals lack any implementation measures to promote or enhance the hospitals information security culture. They argued that hospitals failed to take any practical measures, such as establishing appropriate

procedures, guidelines and processes to eliminate or reduce any threat to the hospitals by maintaining the integrity and confidentiality of patients' medical records. Their hospitals also failed to take appropriate action on employees who abused the integrity and confidentiality of medical records. One of the interviewees explained the following:

> 'The hospital lacks any [implemented] measures to create an appropriate information security culture, and on several occasions, the hospitals failed to take any disciplinary action against employees who abused the integrity and confidentiality of patient records' (Interviewee F).

Another important issue that was explored was the lack of employee training programmes on information security policy. This can be explained by a lack of information security policy, a lack of hospital management's awareness towards information security, and poor attitudes towards information security policy. These issues were explored in several interviews in the three hospitals. One of the interviewees stated the following:

> 'I have been working here in the hospital for over ten years, and I [have] never been trained [in] or seen [a] clear information security policy'
>
> (Interviewee F).

5.5 Communication Systems and Processes

Communication was explored as one of the factors that can either impede or promote a hospital's information security culture. The first issue regarding the current communication system is that it is still traditional and ineffective. Internal communication is still based on personal communication, telephone conversations and paperwork. This type of communication is inappropriate because most employees are busy, and there is no time for this type of communication. This type of communication reflects the hospital's culture. It has

become part of the norm to handle and transfer patient's information using paper work. In this regard, one of the employees stated the following:

> 'The current communication system among the employees is still traditional. It is based on personal communication and paper-based letters' (Interviewee F).

The interviewees indicated that there is a lack of technology used as a tool for internal and external communication within the hospital. They believed that the use of modern technology, such as the latest mobile technologies, enhance the interactions amongst the employees and between the employees and management to facilitate the flow of instructions. They stressed that appropriate and effective communication systems increase understanding, trust, knowledge sharing and respect amongst a hospital's employees. These are critical to promoting and enhancing a hospital's information security culture. It is important to stress that this view was shared and agreed upon by several interviewees from the three hospitals surveyed. One of the interviewees stated that:

> 'the hospital lacks [the] use of technology to enhance and promote employees' interaction to help in knowledge sharing, understanding, building trust, and promoting a positive information security culture' (Interviewee E).

5.6 Saudi National Culture

The main facture of Saudi culture is generally described as the Bedouin tribal culture. This culture has an impact and role on the individual employees' behaviours and interactions within the workplace. The Bedouin culture can be classified as a collectivist culture, wherein the individual puts the interest of the tribe or employer ahead of his or her own interests. For Saudi employees, the values and norms of Bedouin tribes have an impact

on the security of patients' medical records. The interviewees stressed that the employees' passed on patients' medical information to third parties without patient consent based on their Bedouin values and norms. They feel that it is their responsibility to pass on information to comrades from related tribes. This culture-based behaviour has an impact on the confidentiality and integrity of the patients' medical records. One of the interviewees revealed the following:

> 'I think [that] one of the main challenges for the hospital working culture is the employees' Bedouin tribes' vales and norms. It is clear for us [that] this has a serious impact on the information security, especially the patients' medical records. The employee with Bedouin values feels that it is part of their tribe responsibility and duty to pass the information to their tribe comrades' (Interviewee D).

The interviewees stressed that the impact of the Bedouin culture is clear in the administrators' behaviour, but it has less of an influence on the medical and senior medical staff's behaviour. The interviewees argued that this may be due to their education, awareness and attitudes towards information security. It is also important to stress that many senior medical staff members come from different cultural backgrounds that are non-Saudi, and job security for them is a critical factor motivating their behaviour. It seems that non-medical staff members represent the main threat to information security, including administrators, as well as the lower rung of medical staff, such as junior nurses. One of the interviewees explained this problem as follows:

> 'The Saudi cultural-related values and norms have less influence on the senior medical staff behaviour towards information security; this is mainly due to their awareness and attitudes towards information security' (Interviewee F).

5.7 Cultural Diversity in Hospitals

Firstly, it is important to stress that there is a large number of non-Saudi medical staff working for the Saudi health service due to a lack of skill and competence amongst medical staff, especially in nursing. This is due to a lack of recruitment and educational programmes in nursing and, possibly, the attitudes and opinions of the Saudi national culture. Saudi culture is a male-dominant culture that frowns on wives, daughters and sisters working in shifts or working as nurses in hospitals. These attitudes and opinions result in recruiting non-national staff members and creating a multicultural health service.

Based on several interviewees' opinions, cultural diversity within Saudi hospitals has an impact on information security. The interviewees indicated that currently, Saudi National Health Service have several different cultures interacting and working in the hospitals. One of the features of this cultural diversity is the language barrier that exists amongst employees, especially between the medical staff and hospital administrators. On the one hand, some of the employees are not fluent in Arabic; on the other hand, some hospital administrators and managers are not fluent in English. This language discrepancy is one of the main barriers to building trust and understanding amongst hospital employees. Consequently, this has a role and impact on hospital information security. One of the interviewees stated the following:

> 'We have several employees [who] cannot speak Arabic, and we have employees [who] cannot speak English. This makes interaction among the employees difficult. This does not help in building positive information security culture' (Interviewee B).

Another important element of cultural diversity in the hospital is in the employees' own personal cultural background and working cultures. This cultural diversity has also created sub-

cultures within the hospital culture due to the presence of several groups within hospital culture. The diversity in employees' cultures and interactions with other cultures within hospitals is a barrier for effective employee interaction in hospitals. This diversity in cultures impedes effective interaction and communication amongst the employees and has an impact on the security of medical information. One of the statements on this issue was that there is 'a lack of skilled and competent medical staff in SA. The SA National Health Service has a large number of employees from different cultural backgrounds. This diversity has an impact on the hospital culture, employees' interaction, and trust.' (Interviewee F).

5.8 Needs for Change

This section presents the main changes in hospital information security that the interviewees discussed. The section also presents the main reasons to change the hospitals' current cultures.

5.8.1 Needs for Culture Change

Interviewees from the three hospitals agreed that there is a need to change the current hospital information security culture. Regarding the hospital culture, one of the interviewees stated that;

> 'the current hospital culture is one of the main threats to information security, and there is a need to change the current culture' (Interviewee G).

One of the main barriers in changing the hospitals' culture is the lack of appropriate and effective coordination amongst the hospital departments and amongst the hospitals. Change is needed to adopt more effective and appropriate coordination, which will help the flow of information and support employee interactions. Effective coordination will help to establish common policies and strategies to promote information security amongst hospital departments and

amongst hospitals. One interviewee stated that 'the hospital has a large number of medical departments, and the hospital is part of the Saudi National Health Service, Ministry of Health. Therefore, there is a need to change the current coordination to help in enhancing the hospital information security culture' (Interviewee G).

One of the factors explored that has an impact and role on hospital culture is the hospital management structure. The current structure is a rigid, multi-levelled and vertical management style composed of several management layers. This has made the flow of information difficult. It also suggests that the current structure does not facilitate employee interaction. One of the interviewees stated the following in this regard:

> 'The current hospital structure does not recognise the information security culture. The responsibility in developing and enhancing hospital culture is not clear. I believe there is a need to change and identify clearly the responsibility for the hospital culture change'
> (Interviewee G).

Based on several interviewees' arguments, the workplace and rest area environments are some of the areas that need to be changed to enhance and create an appropriate hospital culture. Several interviewees indicated there is a need for better working environments to enhance little control of the employees' and patients' documents. The current rest areas are not appropriate, due to a lack of space and appropriate facilities to enhance employee interaction, share knowledge and build understanding. They argued that an appropriate rest area is important to encourage social interaction and that it also helps to build trust and understanding amongst the employees. They stressed that health service authorities need to change the current working environment and rest areas in hospitals. Interviewees from all three hospitals raised the argument that this may lead one to

believe that the Saudi National Health Service is unaware of the importance and role of rest areas and working environment in building a hospital culture.

5.8.2 Change in Policy

One of the main changes explored in several interviews was the change in current information security policies. The interviewees emphasised that the current policies are mainly generic and out of date; most importantly, they are only focused on accessing control to the information through the utilisation of usernames and passwords. They indicated the need for a change in hospitals' attitudes and opinions towards changing the hospital's information security culture by establishing and implementing appropriate and effective policies.

> 'I would say, based on my experience in several hospitals in SA, with confidence, there is a need for clear information security, especially a policy that takes in consideration the employees' behaviour towards information security'
>
> (Interviewee G).

The current information security policies are out of date and do not reflect the changes from traditional recording to electronic recording, which Saudi Arabia's health service has introduced in several hospitals and will implement throughout the Saudi National Health Service. The current policy does not take into consideration the employee's behaviour or misuse and abuse of the integrity and confidentiality of the hospital's information. The hospitals' current policy should be changed to reflect the hospitals' needs to ensure confidentiality and integrity of information.

> 'We need…a change in current policy, as the current policy fails short to prevent the misuse and the abuse [of] medical information security, especially the patients' medical records. The change should take into consideration the human behaviour, as the current policy mainly concerns [policies] on access control to the system, mainly on using the user names and password abuse. (Interviewee G)

5.8.3 Change in Training Programmes

The interviewees in the three surveyed hospitals explored and stressed that the current training approaches, programmes and strategies need to change to promote and enhance employees' awareness, understanding and knowledge of information security. They stressed that the most appropriate approach to protect the hospital's information is by creating an appropriate information culture by promoting and enhancing the hospital's main actors'—employees'—awareness, understanding and knowledge. This can only be achieved by changing the current training approaches and policies. They agreed that there is a lack of consistent policies: (Interviewee G)

> 'I can [say] strongly [that] the hospital has no approach or policy on promoting and enhancing the employees' opinions, awareness, and attitudes towards the patients' medical record security, the record integrity, and confidentiality'

Other interviewees held stronger views on employee's patient medical electronic records. Saudi Arabia is in the process of implementing electronic patient records throughout the Saudi National Health Service. This represents a shift from the traditional, paper-based patient record towards the use of electronic records. This represents a change in hospital staff working culture, and that change will be strongly associated with a risk that is presented to

patient records. Staff members need to be aware of and trained to protect information security. This can only be achieved through a well-designed and planned training programme. The training programme needs to be focused on promoting information security awareness in an electronic working culture.

> 'The hospital introduced patients' medical records, but there is no plan or policy to make such a change in the hospital working culture. I believe this can be [a] serious challenge to the patient's information security'
>
> (Interviewee G).

5.8.4 Change in Management Opinions and Attitudes

One of the main issues explored in the interviews was the need to change the hospital management's opinions and attitudes. It can be clearly understood that without positive, clear opinions and attitudes from the hospital management, little can be done to promote and enhance an information security culture.

The interviewees were critical in discussing and analysing in depth the importance and need for change in the opinions and attitudes towards the importance and role of information in protecting the National Health Service's medical records. The senior management, such as the Ministry of Health, and hospitals' senior management are the main parties responsible, based on the interviewees, for the current state of the hospital information security culture. This is mainly due to the centralised management and bureaucratic system. One of the interviewees stated:

> ‘In my opinion, as we discuss the hospital information security culture, there is a need to change the hospital management and attitudes—firstly, towards the patient’s medical record confidentiality and integrity and then [their] importance and role [in] creating an appropriate hospital information security culture’ (Interviewee G).

Several interviewees argued and discussed that the changes need to start at the top of the Saudi National Health Service pyramid—namely, the Ministry of Health. They argued that the Ministry of Health needs to establish more effective approaches to promote and enhance hospital environments and provide more support and investment to hospital employees. They felt that the Ministry of Health has fallen short on investing in the human part of health service, although the Ministry has no problem with investing in technology. One of the interviewees stated this issue clearly:

> ‘To be honest, the change needs to be from the top, as the SA National Health Service is centralised and controlled by the Ministry of Health. The Ministry invests in technology to improve the hospitals’ performance, [but they provide] little investment and effort [into] the human part of the services, promoting and enhancing the employees awareness attitudes, knowledge, and their working environment’ (Interviewee G).

The interviewees explored the notion that the health authority needs to change their strategy to ensure job satisfaction in hospitals through establishing appropriate working environments, awareness and knowledge. These help to create positive, productive working cultures and enhance informational medical record security.

The stability of a hospital’s workforce and its management was explored as an important factor in a hospital’s information security culture. The interviewees

argued that a change in culture requires stability from the main actors in the culture over time to help with establishing understanding and trust amongst the employees and between the employees and management. Furthermore, they argued that time was needed to develop a homogeneous culture and that this can only be accomplished by having stability. They also explored the critical importance of having stability in the processes, management structure and working environment of a hospital. The following reflects a common statement regarding stability:

> 'I think [that] the most important factor to improve our working culture is stability [for] the employees and the hospital management. We need time to understand and trust each other, as well as to understand and trust the management. It needs time and effort (processes and policies) to have [an] appropriate hospital culture' (Interviewee G).

5.9 Summary

The main outcomes of the in-depth interviews with key personnel in Saudi Arabian hospitals can be summarised by the following:

- There is a conflict regarding how the health service should be managed. On one hand, the senior medical staff traditionally—and currently—believes that they are the best option to manage the health service's hospitals, due to their medical and management experience. On the other hand, the management team believe that the senior medical staff members should concentrate on medical treatments, where their expertise are needed; management should be those with business and management experience. This may create a conflict between the two groups due to differing opinions.

- One of the main outcomes of the in-depth interviews is discovering the need to change managements' opinions regarding the importance and necessity to enhance and promote health information security, medical record confidentiality and integrity.

CHAPTER 6
CULTURAL INFORMATION SECURITY MODEL

Chapter 6 Objectives

The main objectives of this chapter are as follows:

- To develop principles for cultural information security model.
- To design cultural information security model for SA health service.

Chapter 6 : Cultural Information Security Model

6.1 Introduction

One of the main objectives of this research is to develop an information security culture model. The model is based on identifying the main cultural dimensions and sub-dimensions that contribute to SA health service employees' attitudes towards information security. This section presents and discusses the main model of human behaviour. Information security cultural dimensions have been identified in the literature and fieldwork data analysis. A framework model has been designed and presented based on the behaviour models and the main outcomes of the fieldwork and data analysis.

6.2 Information Security Behaviour models

There are several models for human behaviour in certain actions. This section presents and discusses these models to help develop the framework model for an information security culture for the SA National Health Service.

6.3 IS Culture and Sub-culture Dimensions

National Culture Dimension

One of the dimensions identified in the data analysis is the Saudi national culture. The analyses showed that the national culture plays a role on staff behaviour, such as behaviour towards information security. The national culture has three main sub-cultural dimensions. These sub-cultural dimensions are the working values and norms, tribe values and norms and attitudes and perceptions towards women.

SA Health Services Leadership

Establishing an effective information security culture requires appropriate health service leadership. Leadership has been identified as one of the dimensions that contribute towards staff members' attitudes, which, in turn, contributes to the hospital culture. The leadership has sub-cultural dimensions, such as power sharing, leading by example and developing a vision towards information security within the hospital culture.

Employees' Trust

Trust amongst employees has been identified as one of the dimensions that need to be considered in the hospital culture of information security. The trust can be developed and enhanced by social Interaction, respect and understanding. Trust amongst the employees as well as between the employees and senior management contributes to the hospital information security culture.

Technology Dimension

The hospital's use of technology in its activities and communication contributes to the hospital's culture. The technology dimension contains an Intranet and communication system sub-culture. The intranet can help in promoting and enhancing information security, training and updating staff with new policies, procedures and management operations. On the other hand, technology has become an integral component of communication amongst the hospital medical and non-medical staff members. Communication helps in building staff members' understanding and awareness, and these help in developing trust between the employees and the employers.

Multicultural Interaction

The employees' multicultural background interaction dimensions has sub-cultural dimensions such as language, working values, norms and national culture.

Job Role (Job Satisfaction)

An individual's job role within a hospitals working environment has an impact on the individual's behaviour towards information security, based on the data analysis in the previous chapter. The job role has sub-cultural dimensions including job security and motivation (i.e., job satisfaction) and training.

Developing and Implementing Information Security Policy

Once the hospital develops awareness and understanding of the main drives for its staff members' behaviour, the hospital authority can then develop and implement effective employees' behaviour expectations towards information security policy towards building positive information security culture..

Promoting Information Security Culture

Understanding and awareness of the employees' behaviour towards information security can help in promoting and enhancing the hospital culture. From this research perspective, understanding and analysing staff behaviour will help in recommending practical steps for promoting and enhancing a positive hospital information security culture.

6.4 IS Security Culture Model

A framework model for the information security culture for SA NHS has been developed and illustrated in Figure 6.1. The model is based on human behaviour theory, which is based on the

employees' attitudes towards information security. This plays a major role in the individuals' use and misuse of information in health services. The intention to use patient's information can lead to the actual use of the information. In the hospital, the attitude of staffs' is a key factor in an individual's behaviour, particularly regarding whether he or she discloses information to a third party. The proposed model in figure 6.1 illustrates that six culturally based dimensions contribute to the individual health services' staff members' attitudes towards information security. These six dimensions are as follows: Saudi national culture leadership, trust, technology, multi-cultural interactions in hospitals and job satisfaction. These dimensions contribute to staff attitudes, which lead to the establishment of a distinctive organisation culture. Each dimension identified has its own sub-cultures. The sub-cultural dimensions are the main drives for the cultural dimension, as shown in the figure below.

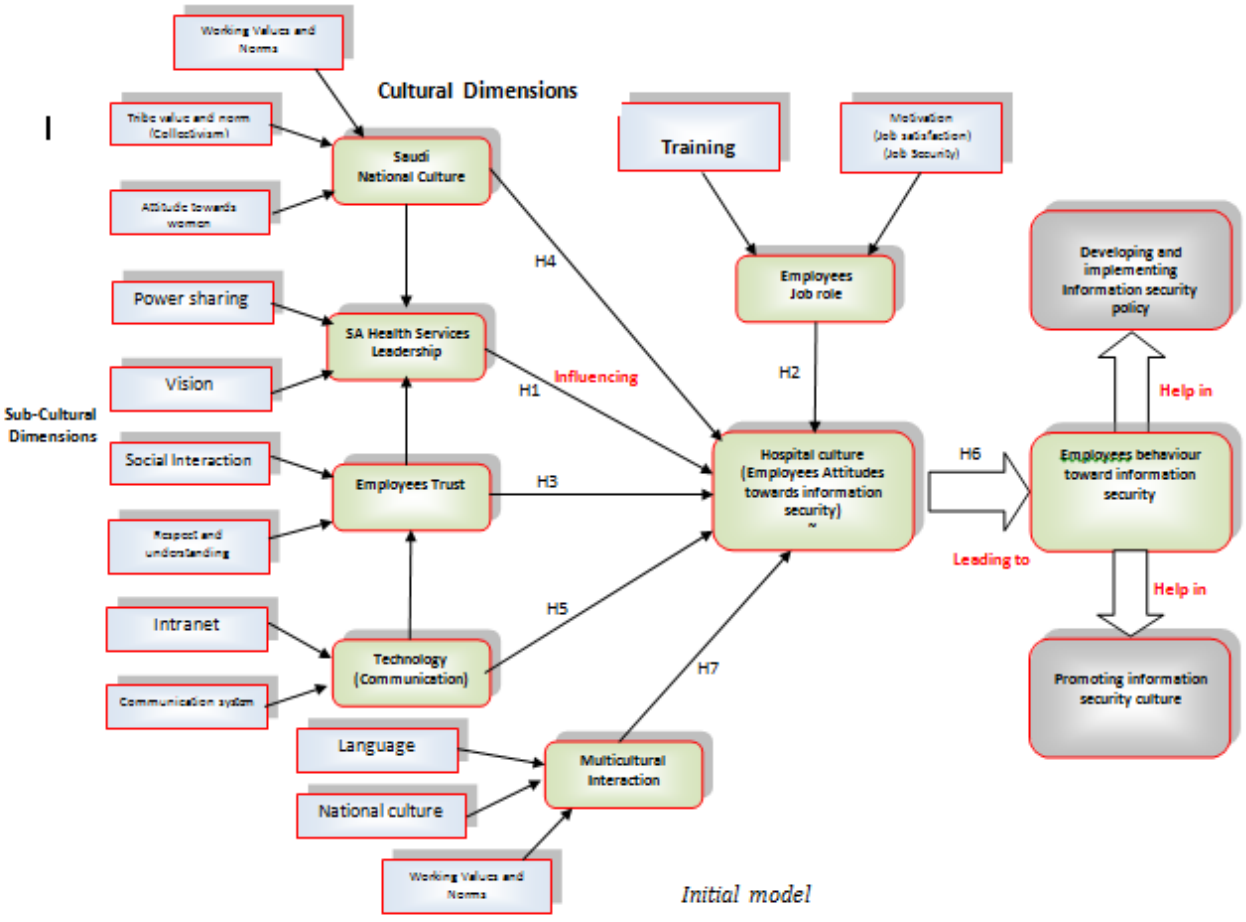

Figure 6-1: Information security culture model

6.5 Summary

This chapter presented and proposed the information security model. The proposed model is based on human behaviour theory and dimensions identified in the literature review as well as data collected for research. The next chapter will evaluate the model by collecting data and information based on the model dimensions.

CHAPTER 7
DATA ANALYSIS: IS FRAMEWORK MODEL EVALUATION

Chapter 7 Objectives

The main objectives of this chapter are as follows:

- To present a data analysis for the evaluation of the developed model.

Chapter 7 **Data Analysis: IS Framework Model Evaluation**

7.1 Introduction

Chapter 6 developed the information security model based on the first fieldwork analysis and the main outcomes of the literature review. The developed model needs to be evaluated and tested to ensure its validity, reliability, practicality and usefulness. A second fieldwork survey carried out between March and May of 2013 collected data and information that is necessary for evaluating the model. The survey included distributing the designed questionnaire, which is in Appendix C, and conducting interviews with key personnel in Saudi health services. The interviews were based on and designed on interview questions discussed in Chapter 5, Appendix D. This chapter presents data analysis of the develop model evaluation.

7.2 Responses

The survey included Saudi nationals and non-nationals to represent the actual hospital working environment. Included in the survey were 64.7% SA nationals (238 out of 368) and (130 out of 368) are non-national. In addition, 58.2% of the respondents were male, and 41.8% were female, as show in the table below**:**

Table 7.1: The respondents' nationality

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Saudi	238	64.7	64.7	64.7
	Non-Saudi	130	35.3	35.3	100.0
	Total	368	100.0	100.0	

7.2.1 Hospitals Surveyed

600 questionnaires were designed and distributed to three hospitals: King Faisal Specialist Hospital and Research Centre, King Fahad Medical City and Specialised Medical Centre Hospital. Two hundred questionnaires were sent to each hospital. The returned and valid questionnaires were 368 questionnaires out of 600, which represents 61.3%. Figure 7.1 shows the number of respondents for each hospital. In addition, the vast majority of the respondents were from King Faisal Specialist Hospital and Research Centre, with 161(43.75%) out of 368. 81 out of 368 were from the Specialised Medical Centre Hospital, representing 22.01%.

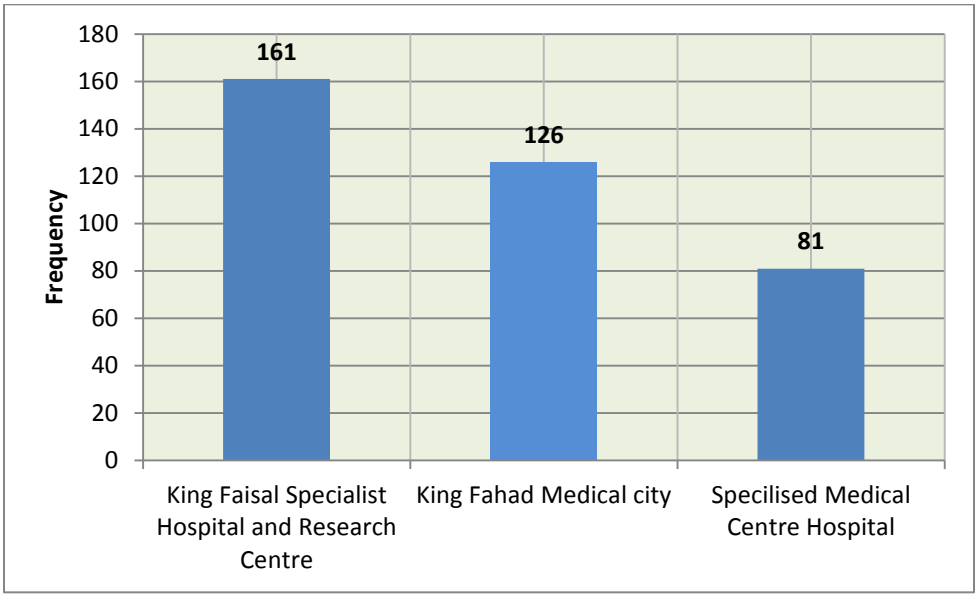

Figure 7-1: Hospitals surveyed

7.2.2 Nationality and Job Role of the Respondents

Saudi Arabian health services use non-nationals to provide services due to the fact that they have a lack of skilled and competent nationals. Figure 7.2 shows the respondents nationality and job role of the respondents'. The figure indicates that the majority (77 out of 141) of the nurses are non-Saudi, and, 25 out of 27, of the medical students are Saudi.

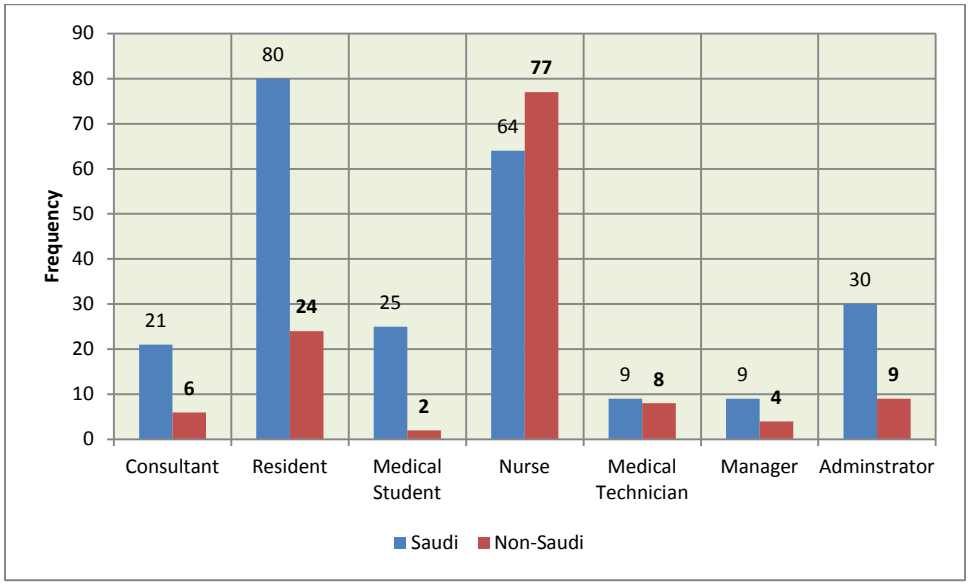

Figure 7-2: Sex and job roles of respondents'

7.2.3 Respondents Experience

Figure 7.3 shows the job roles and the respondents' years of experience. Consultants are the most experienced respondents, and medical students are the lowest. This is mainly due to the experience and job role requirements.

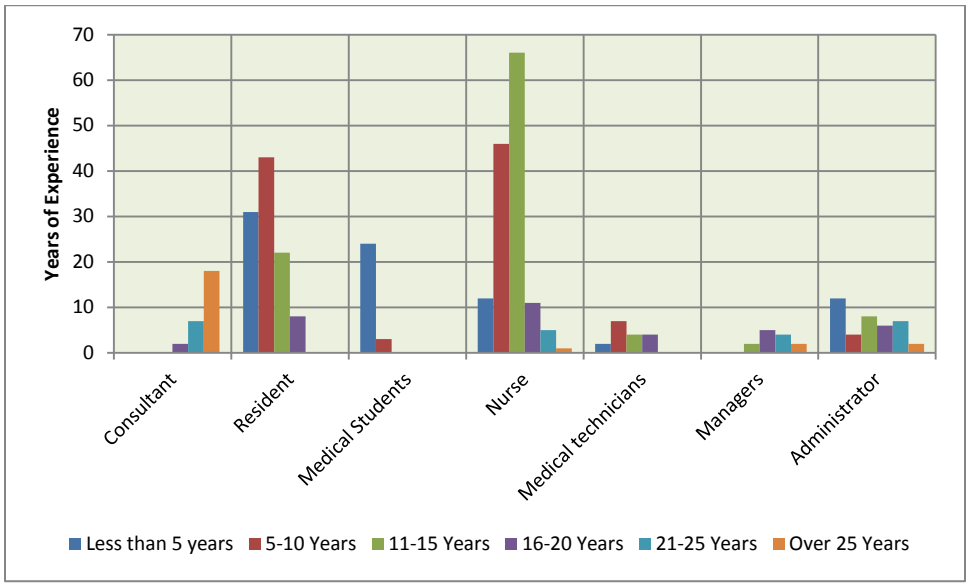

Figure 7-3: Respondents' job roles and years of experience

7.3 Role of Saudi Arabian Culture

Saudi Arabia has a distinctly conservative culture with a special status in the Islamic world due to the holy city of Mecca. The behaviour and attitudes of Saudi Arabia are influenced, to some extent, by Islamic and Arabian culture—namely tribal culture. One of the cultural dimensions of the information security model is the Saudi national culture. This section discusses and assesses the role of this Saudi national culture dimensions on the information security culture.

7.3.1 Tribal Values and Norms

One of the sub-cultural dimensions of Saudi Arabia is the tribal values and norms. Figure 7.4 illustrates the participants' responses towards the following statement: "Tribe values and norms have influenced employees' behaviour towards IS in the hospital". The figure shows that the vast majority, 62.7%, of the participants agreed or strongly agreed with this statement, and only 22.9% strongly disagreed or disagreed.

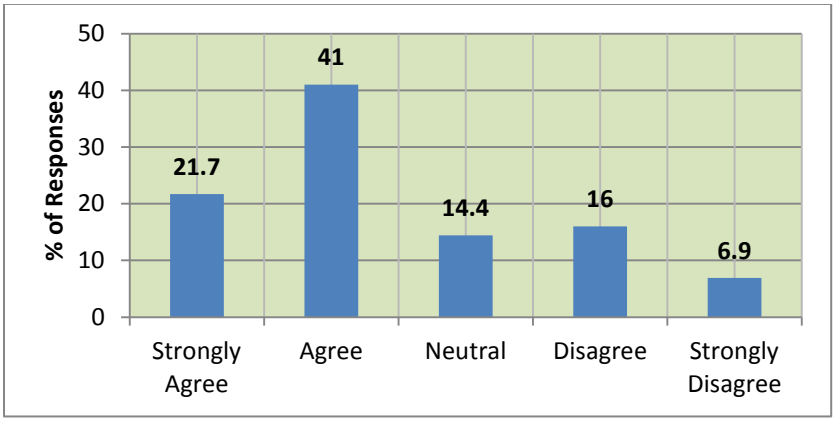

Figure 7-4: Tribal values and norms have influenced employees' behaviour towards IS in the hospital

The interview with key personnel of the three hospitals agreed with the above results. The interviewees stressed that tribal values and norms have influenced Saudi behaviour towards

information security. This seems, in particular, to be due to the Saudi focus on collectivism, rather than individualism. The tribe name and the sense of tribal belonging are stronger than organisation loyalty and interest. One of the interviewees stated the following in this regard:

> 'From my personal observation in my ward, I can say that tribe value has an impact on information security. I [have] observed [that] staff easily gives access to medical information security to his/her…tribe. It seems that [this can be partly attributed]…to the tribe value to stand for each other…[as well as the embarrassment] of not cooperating and refusing a demand for medical information')
>
> (Interviewee J).

7.3.2 Hospital Working Values

Figure 7.5 shows the participants' responses towards the following statement: "Hospital working values and norms have influenced hospital information security". The figure shows that the vast majority, 87.2%, of the participants strongly agreed or agreed with the statement, and only 4.3% strongly disagreed or disagreed with the statement.

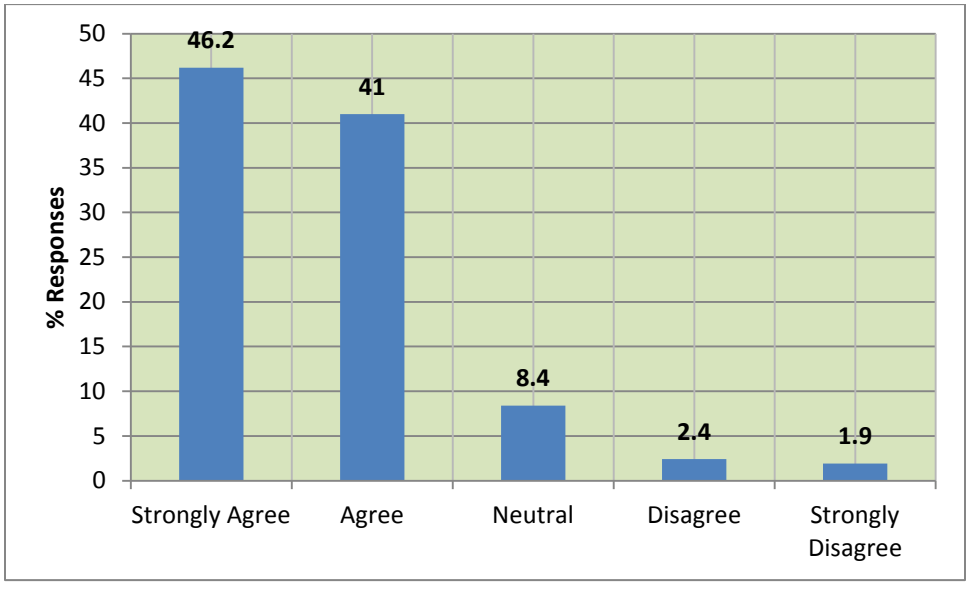

Figure 7-5: Hospital working values and norms have influenced IS

The interviewees agreed with the result. The interviewees, in several statements, indicated that this is one of the main challenges and problems with regards to hospital information security. They indicated that the working values and norms of the hospital have influenced hospital information security. One of the interviewees stated in this regard:

> 'One of the main threats to our information security is the hospital's working values and norms. Passing information to a third party with consent and author, unfortunately, has become part of the hospital norms'
>
> (Interviewee J).

7.3.3 Attitudes towards Women

Figure 7.6 shows the participants' responses towards the following statement: "Tribal values and norms have influenced employees' behaviours towards IS in the hospital". The figure shows that the vast majority, 69.2%, of the participants agreed or strongly agreed with the statement, and only 15.5% strongly disagreed or disagreed.

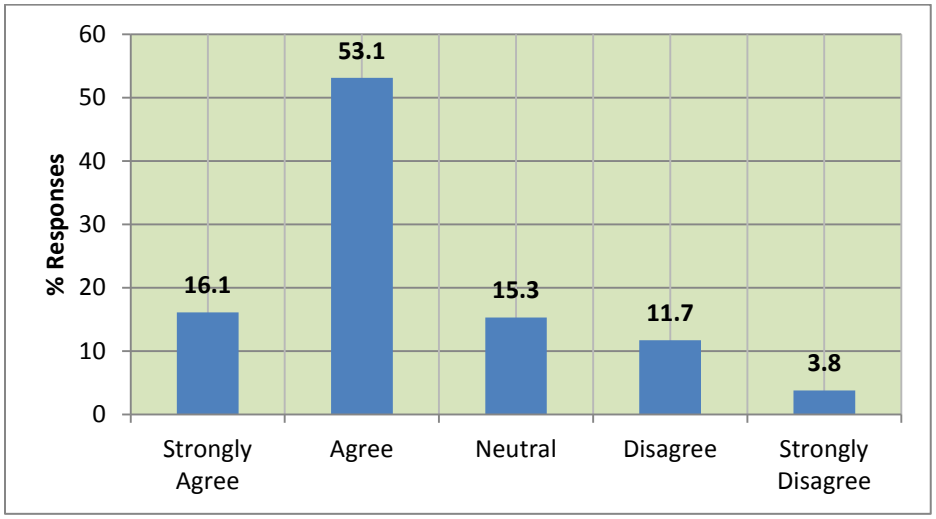

Figure 7-6: Attitudes towards women have influenced hospital information security

Several interviewees indicated that attitudes towards women within hospital interaction environment have influenced information security. They indicated that passing information to female third parties has become the norm. They indicated that male staff members found it difficult to not pass along information to female third parties. They argued that this is part of the Saudi cultural attitudes towards women.

> 'I found [that] males' attitudes towards women have influenced information security. Male staff [are] usually willing to pass information to female third parties compared with male third parties. This [is] possibly due to the attitude towards women in Saudi culture'
>
> (Interviewee A).

7.3.4 SA National Culture and Employees' Attitudes towards IS

The role of Saudi Arabia's national culture on hospital employees' attitudes towards information security is shown in Figure 7.7. The figure shows the vast majority, 70.2% (259 out of 368) of the respondents strongly agreed or agreed that Saudi Arabian national culture has influenced hospital employees' attitudes towards information security, and only 13.9% (51 out of 368) strongly disagreed or disagreed with the statement.

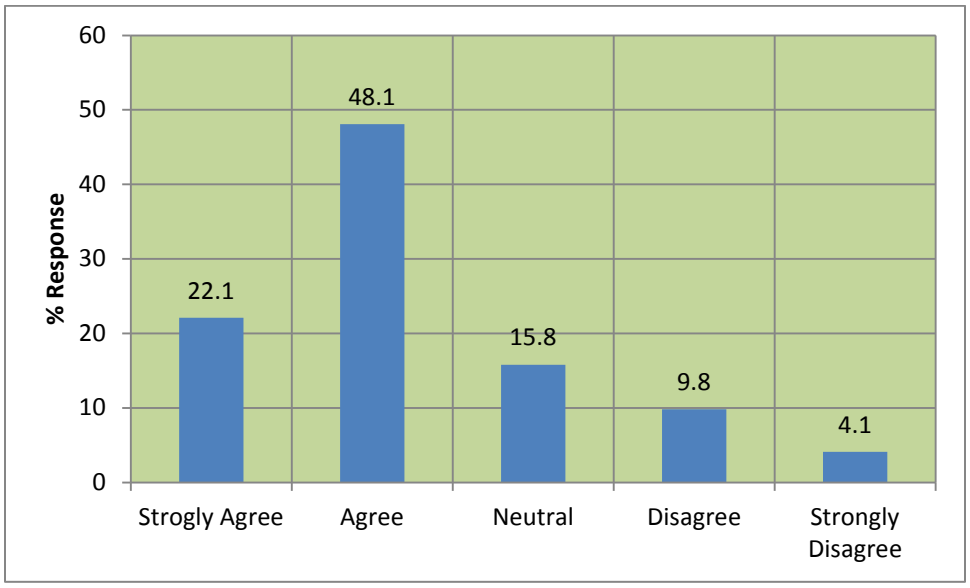

Figure 7-7: SA national culture has influenced hospital employees' attitudes towards IS

The interviewees stated that the SA national culture is clear amongst some of the Saudi employees' attitudes towards information security. It seems that they do not value the security and the need to maintain the confidentiality of the information. They believe, rather, that information security is not the patient's right. They believe that it is the hospitals—and the employee's—right to pass along this information.

> ‘The point I would like to make is the employees’ attitudes towards IS. From discussion and observation with some of my SA colleagues, I would say the value of the medical information is not recognised and [that] some feel that access to the information is the hospital’s and the staff’s right and not the patient’s right’
>
> (Interviewee H).

7.4 Hospital Leadership Style

Hospital leadership style in managing the hospital is one of the cultural dimensions investigated in this research. This dimension aims to investigate the role of leadership styles on hospital culture and the employees’ attitudes.

7.4.1 Saudi National Culture and Leadership

The first leadership sun-dimension analysed is the SA national culture’s influence on leadership style in health services. The vast majority of the respondents, (444 out of 558) 79.6% agreed or strongly agreed with the statement, and only (82 out of 558) 14.7% disagreed or strongly disagreed, Figure 7.8.

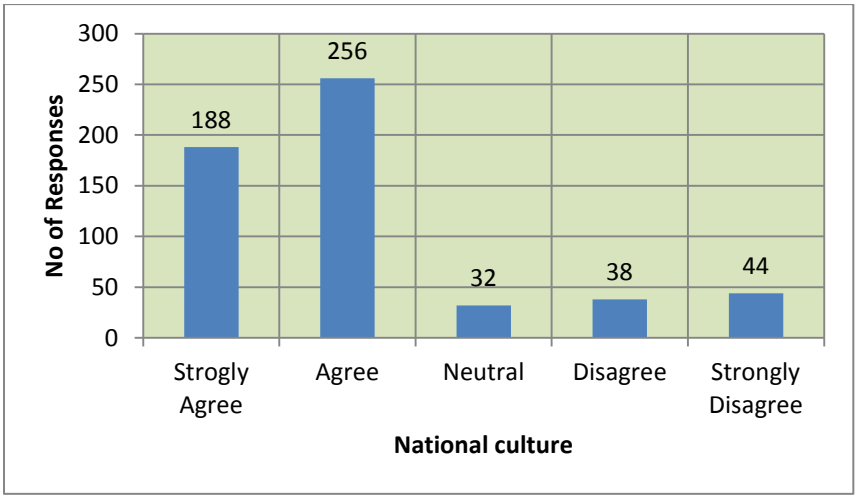

Figure 7-8: National culture has influenced leadership styles in SA health services

The interviewees believed that it is the hospitals —and the employee's—right to pass along confidential information. One of the dimensions explored is the type of communication preferred by employees as part of their daily activities. They stressed in various statements that direct, face-to-face communication is the most effective approach in solving problems and passing along information.

> 'I would say [that] there [is a] trace of SA culture on the leadership management style. The leadership still prefers direct communication, face-to-face interaction, rather than using electronic or email instruction and passing information, possibly [due to a] trust issue, in solving work-based problems. It is part of SA culture [to prefer] face-to-face communication'
>
> (Interviewee G).

7.4.2 Leadership and Sharing Power

Figure 7.9 shows responses towards the following statement: “Hospital leadership style that includes sharing of power in managing the hospital has influenced the information security”. The figure shows that the vast majority, 80.9%, strongly agreed or agreed with this statement, while 10.6% were neutral, and only 8.5% disagreed or strongly disagreed with the statement.

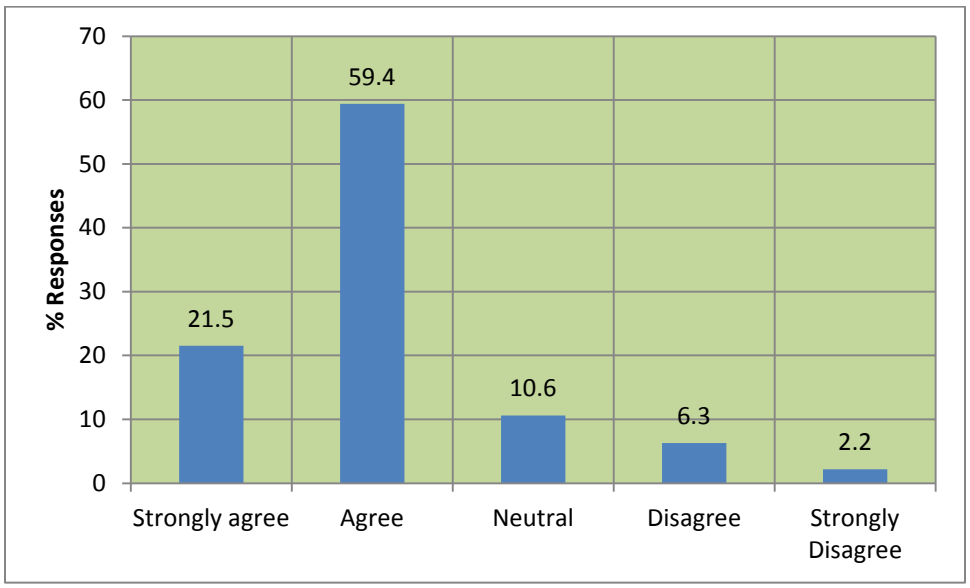

Figure 7-9: Hospital leadership style that includes sharing power influenced the IS.

The role of leadership style, such as in sharing power, with the hospital’s employees was analysed to investigate whether sharing power has an impact on the hospital’s information security. The interviews indicated that the leadership style is centralized, with no or little sharing of power in managing the hospital. The interviewees believed that this has influenced both complying and monitoring compliance and ensuring information security. They argued this is mainly due to leadership style and power, without allowing others to contribute and share power or to contribute to a hospitals decision-making process.

One of the individuals stated the following regarding this topic:

> 'I believe with no doubt [that] sharing power by giving us more responsibility and decision making [opportunities]; this, with no doubt, will help [in] improving the information security compliance and monitoring any misuse or handling [of] the information. BUT, as I said earlier, the leadership style is centralised power, with no or little sharing in managing the hospital'
>
> (Interviewee G).

7.4.3 Leadership and Sharing Vision

Figure 7.10 indicated that the majority of the respondents, 54.5% strongly agreed or agreed that the hospital leadership sharing its vision with employees towards information security influenced the information security culture. Only 14.5% disagreed or strongly disagreed with the statement. Just over a quarter of the respondents, .31% remained neutral.

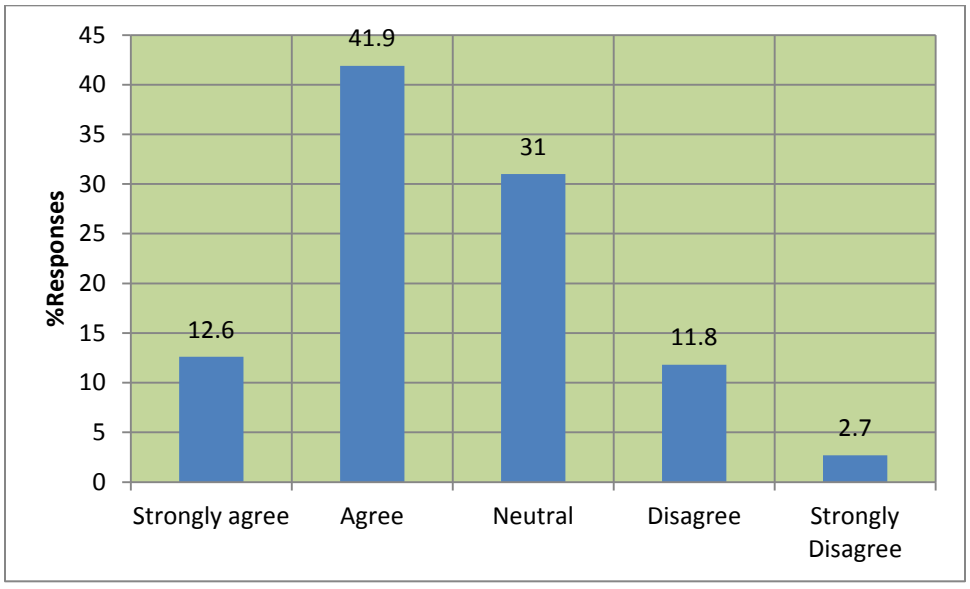

Figure 7-10: Leadership sharing vision influenced the IS culture.

The interviewees made several statements that revealed that the vision of health service is mainly decided and implemented by central government, with little or no input by hospital leadership and management. They argued that at this stage, there is little vision sharing and strategic planning for medical information security. The main worries are the changing forms of information from traditional to electronic means. There is a need for quick responses in order to control and monitor medical information. One of the relevant statements in this regard is as follows:

> 'The vision is a long strategic planning and may not have any immediate impact on the information security. It is possible [that it] has an impact on long-term strategic planning on handling and transmitting medical information throughout the system. It is also the vision of health services [that is] usually controlled by central government'
>
> (Interviewee F)

7.4.4 Leadership and Information Security

For this research, we analysed hospital leadership's influence on information security, and the analysis showed that the vast majority of the respondents, 78.4%, strongly agreed or agreed with the statement hospital leadership has influenced information security. See Figure 7.11. The figure indicates that only 12% strongly disagreed or disagreed with statement, and 9.6% were neutral.

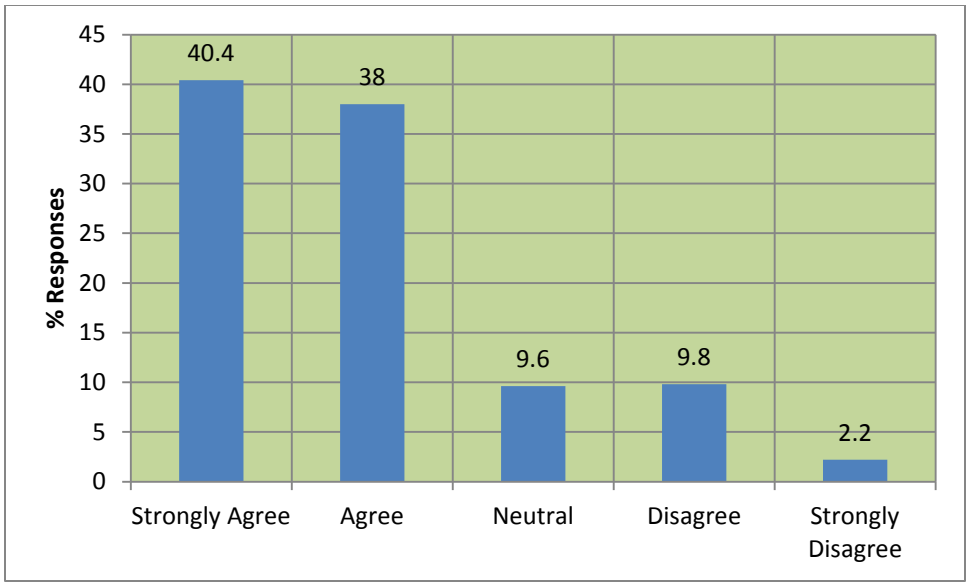

Figure 7-11: Leadership attitudes influenced the IS culture

Almost all of the interviewees indicated that the hospital leadership plays a critical role in hospital information security. One of the statements that an individual made in this regard is as follows:

> 'There is no doubt for me that the hospital leadership plays a major role in the hospital information security. The leadership can influence information security policy, training, and promoting positive hospital culture with positive information security values and norms'
>
> (Interviewee D).

7.4.5 Leadership and Employees' Attitudes

Figure 7.12 shows that the vast majority, 79.2% (289 out of 365) of the respondents, believe that SA hospitals' leadership styles have influenced hospital employees' attitudes towards information security. Only 8.2% (30 out of 365) strongly disagreed or disagreed with the statement. 12.6% (46 out of 365) of the responses were neutral towards the statement.

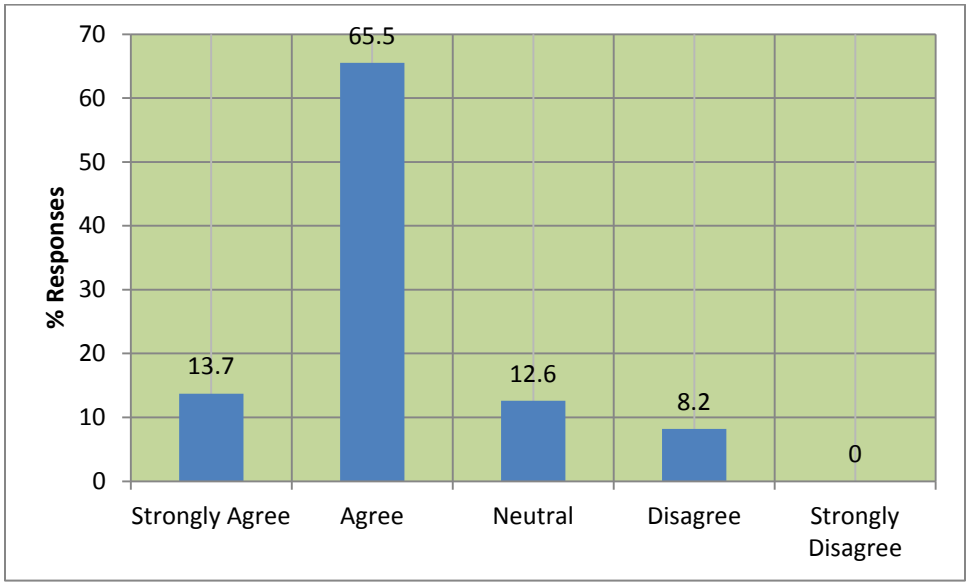

Figure 7-12: Leadership style has influenced employees' attitudes towards IS

The interviewees expressed their opinions on the role of hospital leadership regarding information security. They indicated that the employees' attitudes are the outcome of workplace activities, working values and norms and information security policy strategy and implementation. In all of these areas, the leadership plays a major role. One of the statements in this regard spoke to the enforcement and enhancement of such attitudes.

> 'There is no doubt for me our hospital leadership plays an important role towards the information security. The role comes out from the leadership attitude and belief on the need and the importance of the hospital information security. For me, the leadership needs to be led by example [regarding] information security behaviour and attitudes'
>
> (Interviewee H).

7.5 Trust

Trust is one of the culturally based elements identified in the literature, and it is also one of the dimensions of the proposed information security model. The respondents were asked five questions relating to trust in order to identify and assess the role of trust in information security in hospitals. This section presents an analysis of the role of trust on information security.

7.5.1 Employees' Trust and Information Security

Figure 7.13 shows the responses towards the following statement: "Trust amongst the employees has influenced the information security". The vast majority, 82.3% (303 out of 368) of the respondents strongly agreed or agreed with the statement, and only 4.9% (18 out of 368) disagreed or strongly disagreed with the statement.

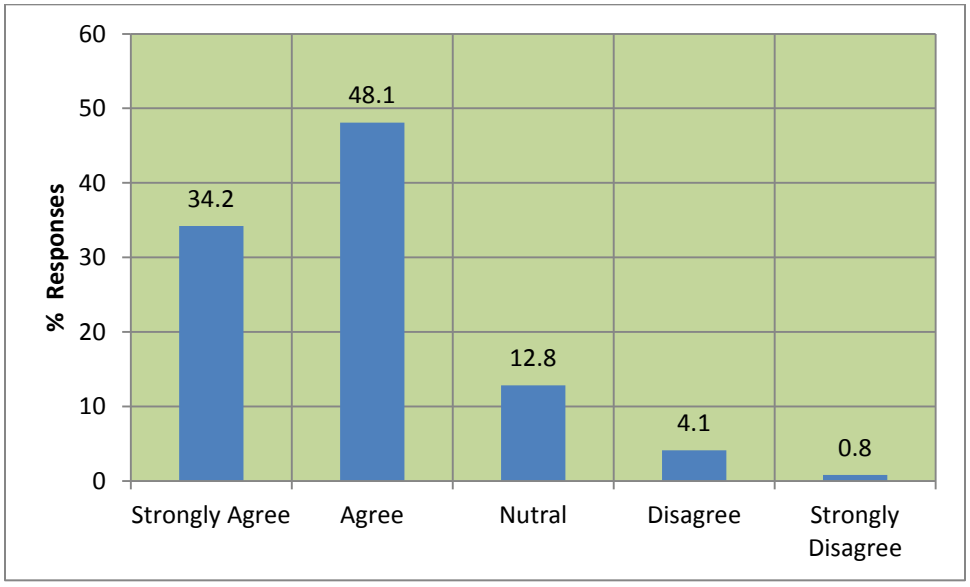

Figure 7-13: Employees' trust influences hospital employees' attitudes towards IS.

The trust amongst the employees was found to be influencing attitudes towards information security. Trust amongst the employees helps in information exchange and transmission as well

as knowledge sharing. This has a profound impact on the employees regarding information security. In fact, one of the interviewees claimed,

> 'I found trust among the nurses helped in building a good attitudes towards information security'.

7.5.2 Employees and Hospital Management Trust

Figure 7.14 shows the responses towards the following statement: "Trust between the employees and the management has influenced the information security". The vast majority, 81.2% (299 out of 368), of the respondents strongly agreed or agreed with the statement, and only 8.7% (32 out of 368) disagreed or strongly disagreed with the statement.

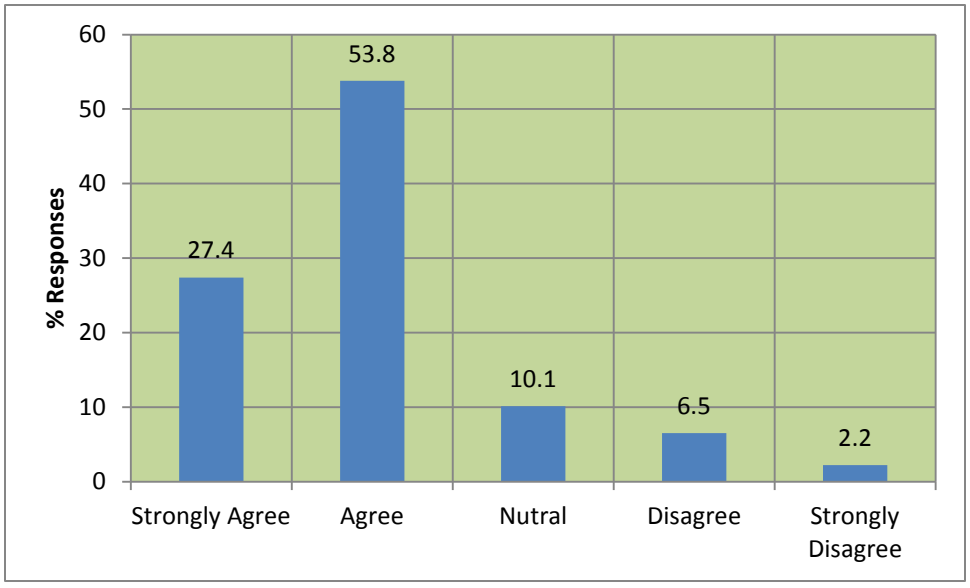

Figure 7-14: Trust between the employees and the management influences IS culture.

Trust between the hospital employees and the hospital was also explored as one of the factors for information security in the survey of the three hospitals. The discussion focused on a lack of trust leads to non-compliance of any information security policy, instruction or order. The

interviewees have also claimed that a lack of trust can lead to not implementing the hospital's instructions and roles, and this can certainly influence the hospital's working culture. Another important issue raised is that the lack of trust, in some cases, had led to tension and stress in relationships and has influenced the hospital's performance and its operations. Undoubtedly, this has also significantly affected the hospital information security.

> 'Lack of trust between us at this hospital and [with] our management has led sometimes to stress and tension. It has influence[d] employees' behaviour in the hospital and, in several cases … [leading to employees'] not respecting the management's decisions, instructions and plans'
>
> (Interviewee C)

7.5.3 Employees' Understanding

Figure 7.15 shows the responses towards the following statement: "Understanding between the employees has influenced information security." The vast majority, 60.2% (221 out of 368), of the respondents strongly disagreed or disagreed with the statement, and only 21% (77 out of 368) strongly agreed or agreed with the statement.

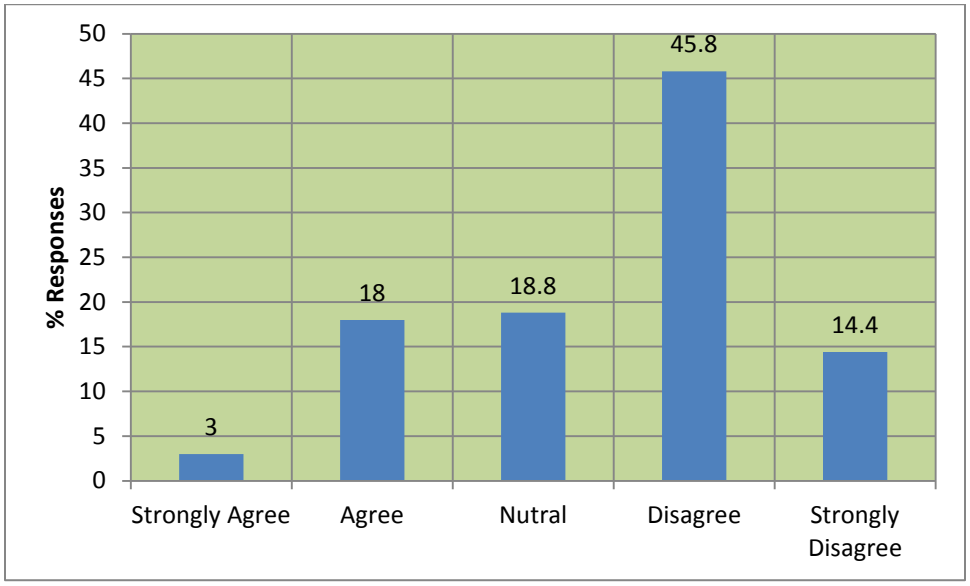

Figure 7-15: Understanding between the employees has influenced the IS.

Understanding amongst employees was explored and discussed with the interviewees to assess its role in developing a culture focused on information security. It was clear from the interviews that understanding amongst the employees is needed to have a healthy and productive hospital culture. Understanding amongst the employees was explored as an important factor to facilitate and enhance employees' interactions, policy compliance, trust and ability to develop a productive and efficient hospital culture. The interviewees explained that understanding helps

to facilitate the flow of information. They argued that understanding could play a role in information security. One of the employees, for example, stated the following:

> 'My observation [is that] understanding among ourselves helped us to do our job better, [made] us happy and created [a] positive and productive working culture. Understanding helped to enhance our trust and compliance as well as enhance information security'
>
> (Interviewee B)

7.5.4 Social Interaction and Trust

Figure 7.16 shows the responses towards the following statement: 'Social interaction among the employees has influenced the information security'. The vast majority, 70.9% (261 out of 368) of the respondents strongly agreed or agreed with the statement, and only 13.8% (51 out of 368) strongly disagreed or disagreed with the statement.

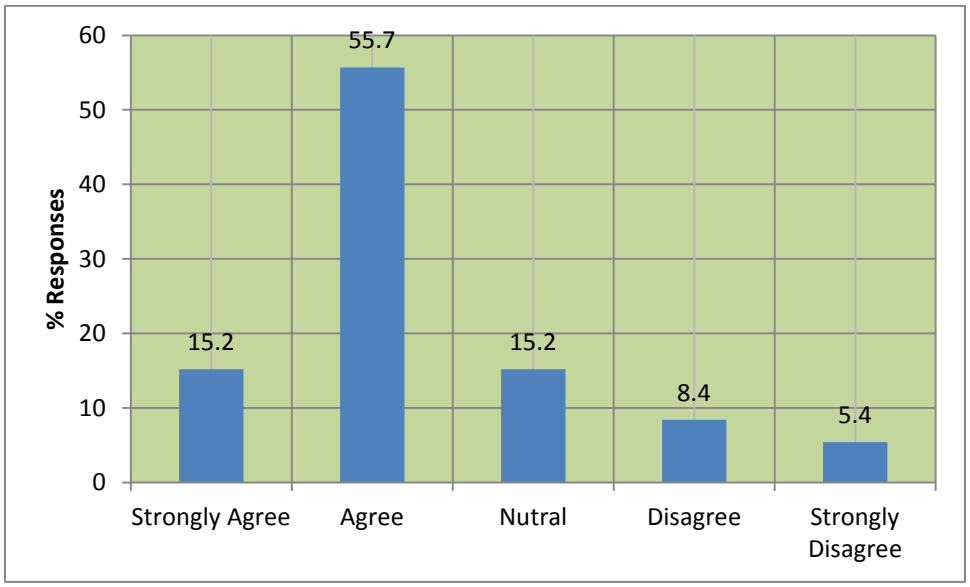

Figure 7-16: Social interaction among the employees has influenced the IS.

In several interviews, we held discussions on social interaction to assess the employees' social interaction on information security in the hospital's working environment. The interviewees explained that social interaction helps develop an understanding of others' cultural backgrounds, values, and beliefs. They also explained that social interaction helps in developing and enhancing trust amongst the employees. This demonstrates that social interaction can help in improving and enhancing information security through building positive staff relationships, trust, respect and understanding. One of the interviewees explained the following:

> 'I found my social interaction with the Saudis helped me [with] understanding their values, culture and beliefs. It also helps them to understand my cultural background, values and beliefs. I think this helped [in] building our trust and building positive relationships. In my view, this helps in the hospital information security'
>
> (Interviewee F)

7.5.5 Employees' Trust and Attitudes towards IS

Figure 7.17 shows the responses towards the following statement: "Employees' trust among themselves has influenced hospital employees' attitudes towards information security". The vast majority, 82.1% (302 out of 368), of the respondents strongly agreed or agreed with the statement, and only 4.4% (16 out of 368) strongly disagreed or disagreed with the statement.

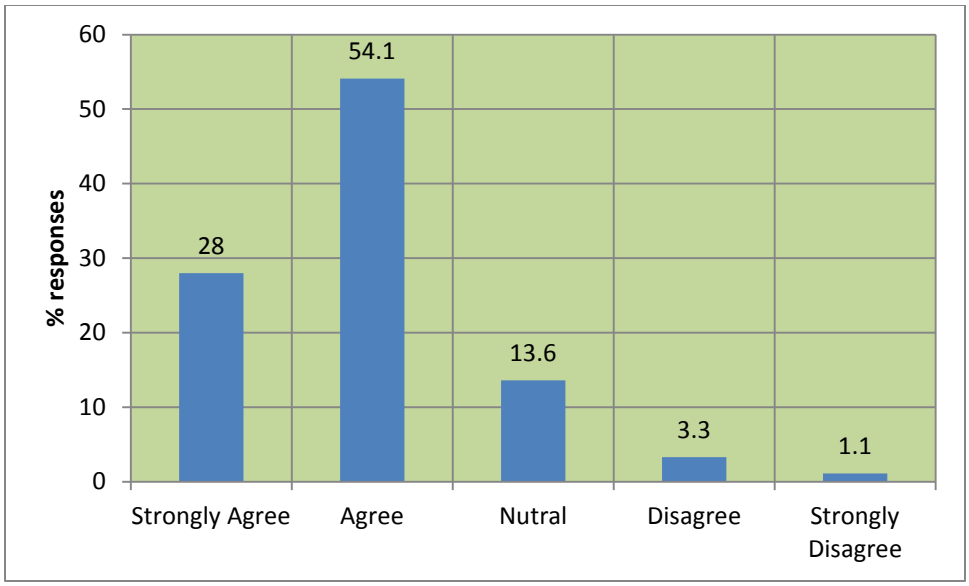

Figure 7-17: Employees' trust influenced hospital employees' attitudes towards IS culture.

One of the questions that was raised in the interviews was the role of trust amongst employees' themselves and the attitudes towards information security. They argued that attitudes were outcomes of several factors, such as the trust amongst the employees. Trust amongst the employees helps in building positive attitudes towards information security. The trust amongst employees also helps in building a positive hospital security culture. One of the interviewees stated on this issue:

> 'I would like to say with confidence that trust among ourselves helps the hospital operations and improve efficiency of our activities. One of the factors, I would say is improving and enhancing information security is the trust. Trust is a critical factor for hospital culture'
>
> (Interviewee F)

7.6 Role of Technology

Hospitals in SA are adopting the use of technology to facilitate managing their operations, as well as improving patients' health care. The use of technology has given users of technology the power to access information regarding patients and employees.

Figure 7.18 indicates the responses towards the role of technology on information security in the hospital. The vast majority, 76% (280 out of 368), of the respondents strongly agreed or agreed with the statement, and only 22.9% (84 out of 368) strongly disagreed or disagreed with the statement.

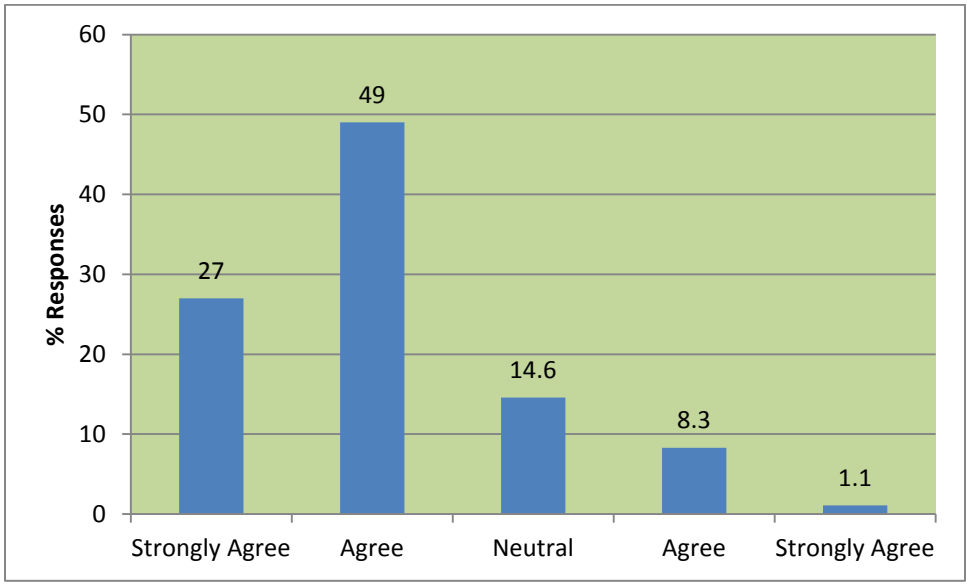

Figure 7-18: Role of technology on information security culture.

One of the interviewees indicated that the use of technology could be a threat to information security as well as the privacy of patients and employees' personal data. This can be serious,

with the absence of an appropriate data protection act to protect patients' and employees' personal information. One of the interviewees stated,

> 'The use of technology has improved our operation, but it has also given users access that may influence patients' and employees' privacy'
> (Interviewee E).

7.6.1 Hospital Intranet

Figure 7.19 shows responses towards the following statement: "Hospital intranet has influenced the information security culture". The vast majority, 51.5%, of the respondents strongly disagreed or disagreed with the statement, and 30.5% strongly agreed or agreed with the statement. 18.5 were neutral.

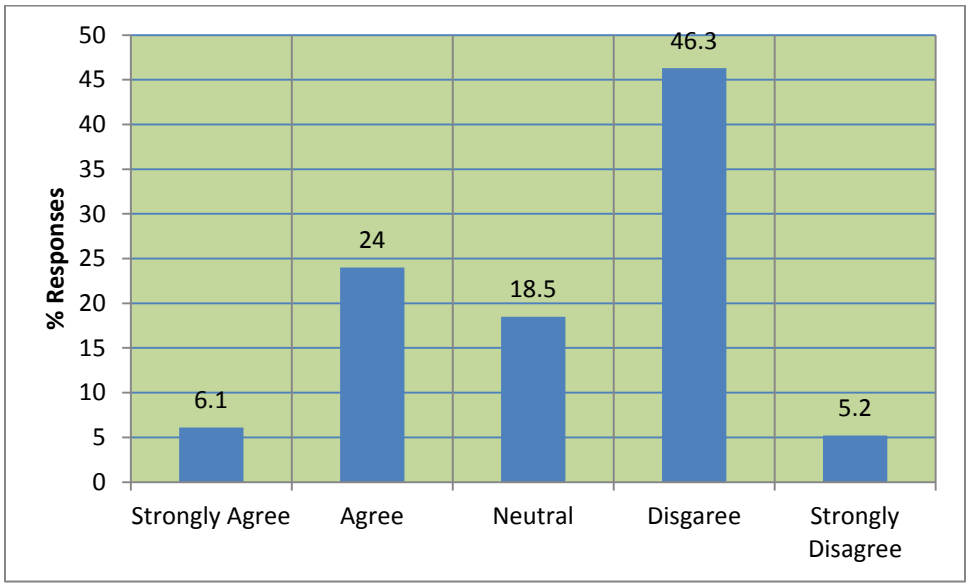

Figure 7-19: Hospital intranet has influenced the information security culture.

Intranet plays an important role in managing an organisation's activities and informs and updates staff regarding the organisation's activities, rules and decision-making. It helps employees to communicate with the organisation management and vice versa. The data analysis indicated that

hospital's intranet is still not used effectively to support hospital staff and promote and enhance hospital information security culture. One of the interviewees stated the following regarding this issue:

> 'Although we claim, as a hospital, that we have intranet, from personal experience for the last ten years, I could say with confidence that our intranet is not effective and that it cannot play a major role in information security'
>
> (Interviewee E)

One of the interviewees also stated the following on this issue:

> 'In principle, the hospital intranet can play a role in enhancing hospital information security, but in this hospital, [it] is minor factor in the processes
>
> (Interviewee A)

7.6.2 Hospital Communication System

Figure 7.20 shows responses towards the following statement: "The hospital communication system has influenced the information security". The vast majority, 77.2% (284 out of 368), of the respondents strongly agreed or agreed with the statement, and only 13.3% (49 out of 368) strongly disagreed or disagreed with the statement.

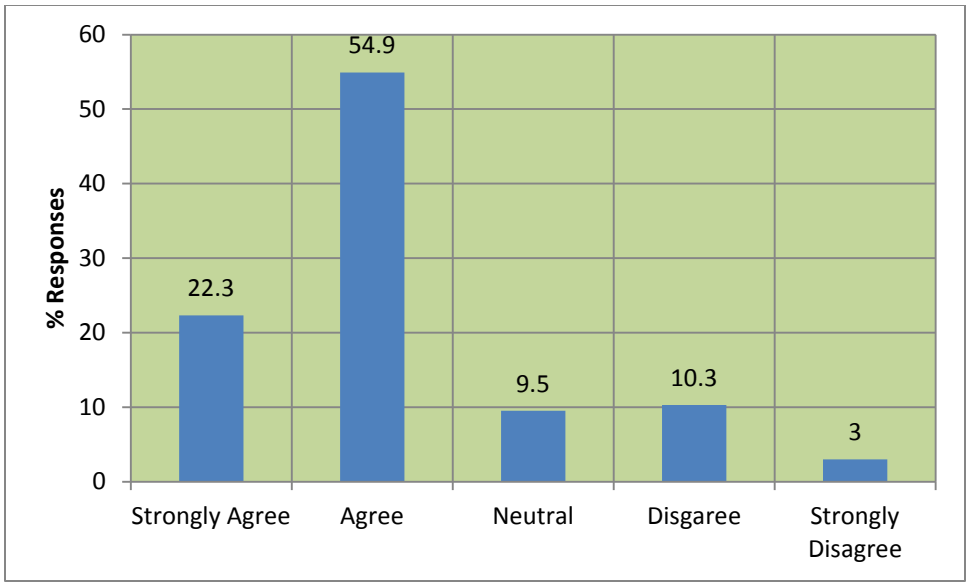

Figure 7-20: Hospital communication system has influenced the IS.

Several interviewees stressed that a hospital's communication plays a major role in helping to improve the information security culture. They stressed that an effective communication system helps with the process of interaction. Interactions between employees help in developing respect, understanding and knowledge sharing. One of the interviewees stated the following on this issue:

> 'I have no doubt that effective and appropriate communication systems in the hospitals help in improving information security. They help in teams' and individuals' interactions'
>
> (Interviewee A)

In addition, other interviewees stated the following on this issue:

> 'Communication is a process [that] helps in building understanding, awareness and compliance of information security'
>
> (Interviewee B)

7.6.3 Electronic Information

Figure 7.21 shows the responses towards the following statement: “The electronic information system has influenced the information security”. The vast majority, 81.2% (299 out of 368), of the respondents strongly agreed or agreed with the statement, and only 9.5% (35 out of 368) strongly disagreed or disagreed with the statement, while only 9.2% remained neutral on the issue.

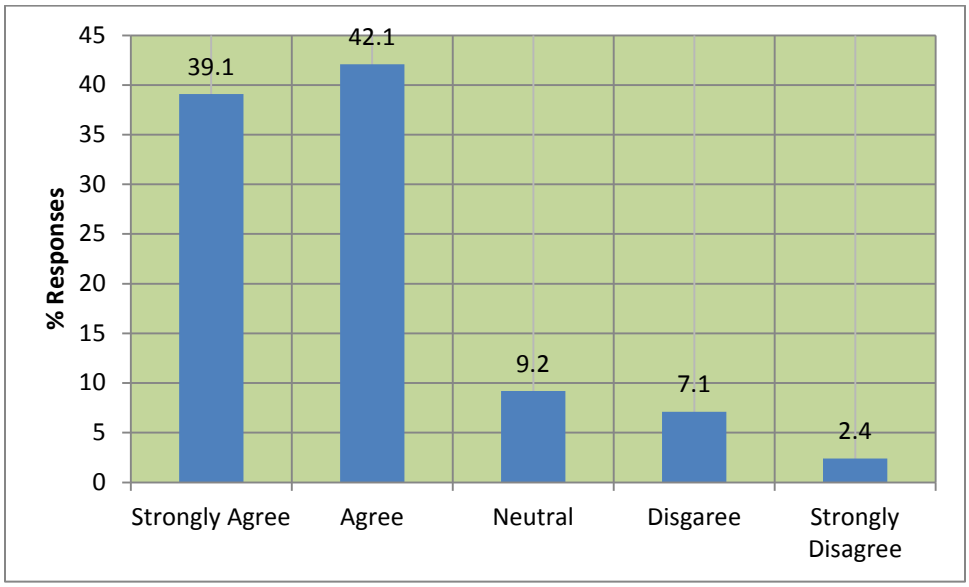

Figure 7-21: Electronic information system has influenced the IS.

The interviewees also explained, to some extent, the problems associated with electronic medical information from an information security culture point of view. One of the interviewees stated the following on this issue:

> ‘Working in electronic medical information form creates a problem. The threat is [that it is] easy to transmit and receive the information. It also facilitate[s] in accessing the information’
>
> (Interviewee E)

7.6.4 Use of Technology

Figure 7.22 shows the responses towards the following statement: "Use of technology in the hospital has influenced information security". The majority, 46.5% (171 out of 368), of the respondents strongly agreed or agreed with the statement, and 43% (158 out of 368) strongly disagreed or disagreed with the statement, while only (39 out of 368)10.6 % remained neutral.

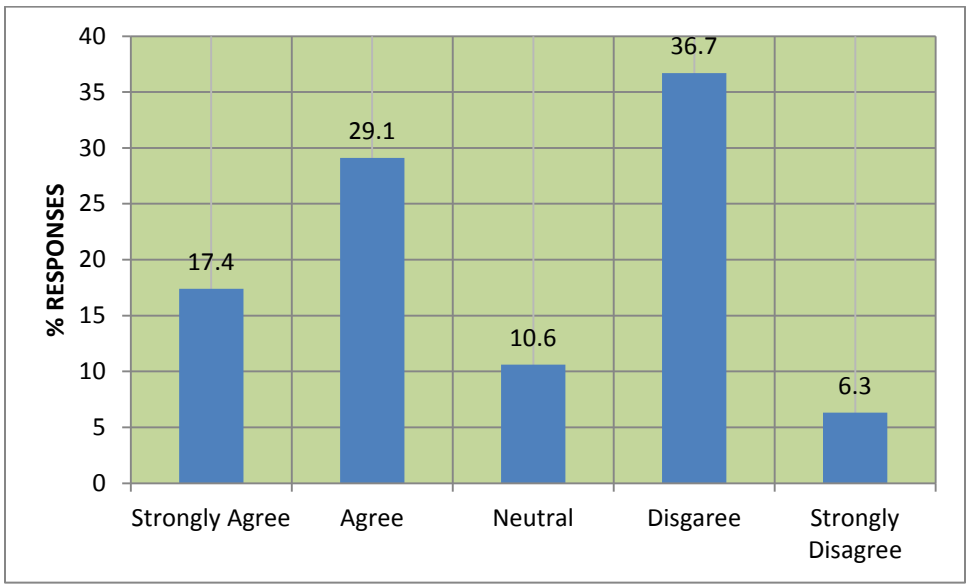

Figure 7-22: Use of technology in the hospital has influenced the information security.

Interviewees stated that the use of technology as a tool in managing and handling information within the hospital could be problematic as it pertains to information security culture. Technology gives employees access to information, and that can be a problem from the information security point of view if the use of information is abused. Regarding the use of technology, one of the interviewees stated the following:

> 'Use of technology in the recording and transmitting [of] hospital information can be a threat to information security'
>
> (Interviewee F)

7.6.5 Technology and Employees' Attitudes

Figure 7.23 shows the responses towards the following statement: "Use of technology in the hospital has influenced hospital employees' attitudes towards information security". A total of 46.5% (171 out of 368) of the respondents strongly agreed or agreed with the statement, while 43% (158 out of 368) strongly disagreed or disagreed with the statement, and only 10.6% (39 out of 368) remained neutral.

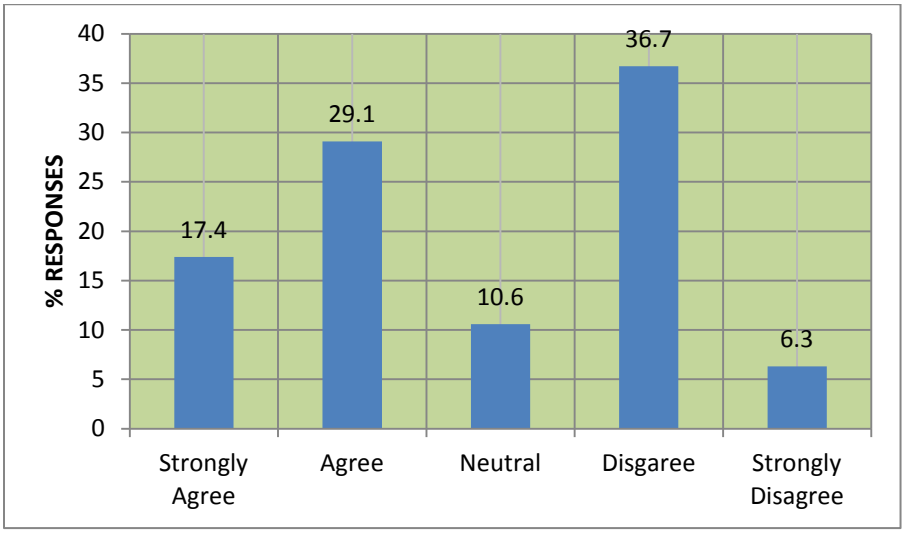

Figure 7-23: Technology influences employees' attitudes towards IS culture

Employees' attitudes towards the use of technology on the hospital's operations and management were explored, to some extent, in the interviews with key hospital staff. They believed that employees' attitudes towards technology definitely had an impact on their handling and managing of information efficiently and effectively. One of the interviewees stated the following:

> 'No doubt, the attitude towards technology is critical on the employees' behaviour towards information security'
>
> (Interviewee F).

7.6.6 Hospital Communication and Trust

Figure 7.24 shows the responses towards the following statement: "The use of technology in hospitals has influenced hospital employees' attitudes towards information security".

The vast majority, 66.8% (245 out of 367), of the respondents strongly agreed or agreed with the statement, and 29.2% (73 out of 367) strongly disagreed or disagreed with the statement, while only 4.1% (49 out of 367) remained neutral. It is, thus, evident that hospital communication systems have influenced the employees' trust in information security.

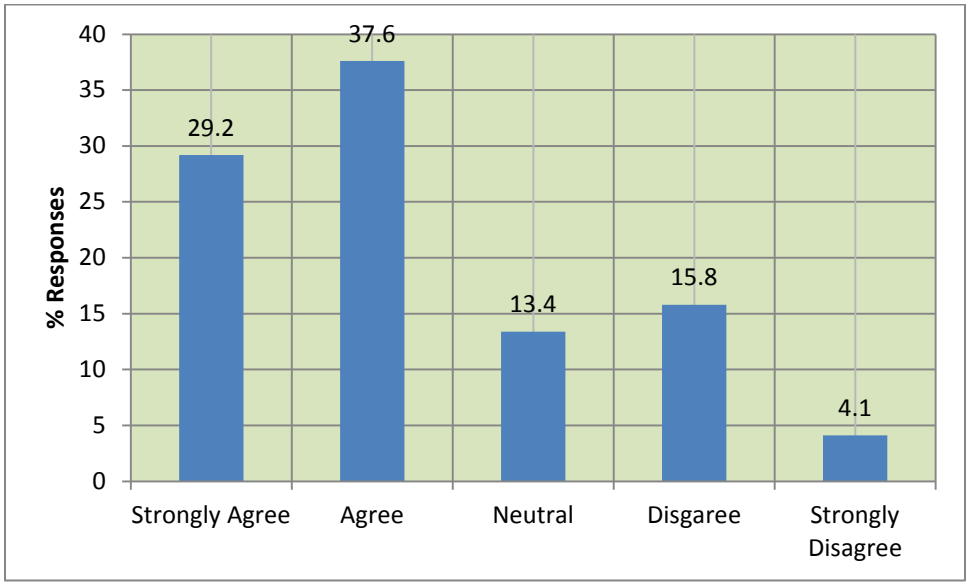

Figure 7-24: Communication system influenced the employees' trust in IS.

One of the interviewees stated the following on this issue:

> 'The hospital communication system has an important and critical role on the hospital culture, and this, without any doubt, plays a major role in the hospital information security'
>
> (Interviewee F).

7.7 Role of Multicultural Interaction

This section presents an analysis of multicultural interactions within the organisation.

7.7.1 Role of Languages

Figure 7.25 shows the responses towards the following statement: "Employees' different languages have influenced information security".

The vast majority, 77.2% (284 out of 367), of the respondents strongly agreed or agreed with the statement, and 13.3% (49 out of 368) strongly disagreed or disagreed with the statement. Only 9.5% (35 out of 368) remained neutral.

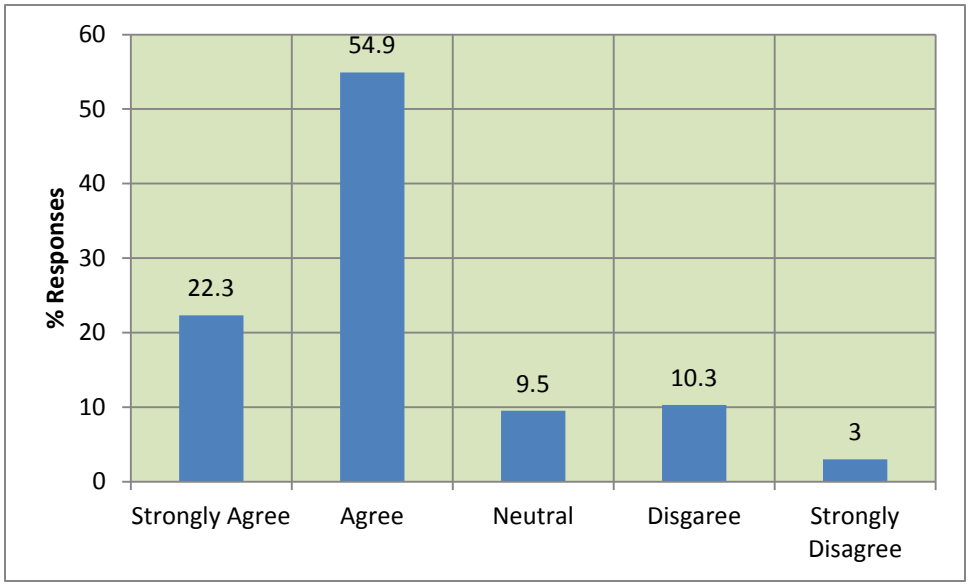

Figure 7-25: Different languages have influenced the information security.

One of the interviewees argued that use of different languages among the employees have helped in developing understanding and trust among the employees through facilitating appropriate communication process. The interviewee stated in language issue:

> ‘As you observing in our hospital, different languages and Arabic accents are used as a tool in the communication process. I would say [that] language helps in understanding, respecting [one another and] passing information. Knowledge sharing and trust amongst the employees [are important]. So I can argue indirectly [that]…language is [an] important factor in our hospital information security’
>
> (Interviewee C)

7.7.2 Diversity in National Culture

Figure 7.26 shows the responses towards the following statement: “Diversity of nationality and culture of the employees has influenced information security”. The vast majority, 81.2% (299 out of 368), of the respondents strongly agreed or agreed with the statement, while 16.3% (60 out of 368) strongly disagreed or disagreed with the statement, and only 2.4% (9 out of 368) remained neutral.

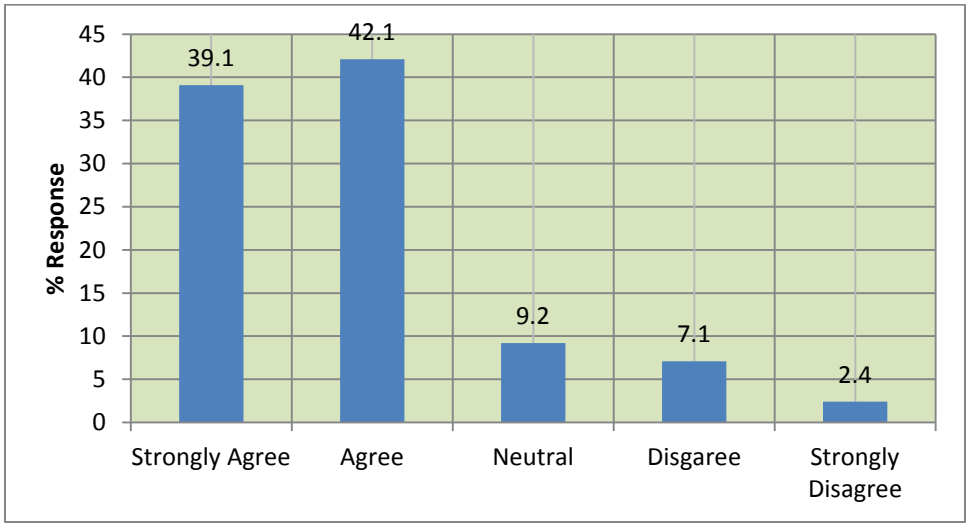

Figure 7-26: Diversity of national culture influenced the IS culture

Diversity of national culture influence the information security was clear on one the interviewees’ statement. The interviewee stated in this regard:

> ‘We have over ten nationalities working in this hospital, and they are coming from different cultural backgrounds. In my opinion, an individual’s cultural background and culture play a role on the individual’s roles and responsibilities. I found different cultural backgrounds have influenced complying with information security instruction and policy’
>
> (Interviewee B)

7.7.3 Diversity in Working Values and Norms

Figure 7.27 shows the responses towards the following statement: “Diversity in working values and norms of the employees has influenced information security”. The vast majority, 83.5% (307 out of 368), of the respondents strongly agreed or agreed with the statement, and 7.3% (27 out of 368) strongly disagreed or disagreed with the statement, while only 9.2% (34 out of 368) remained neutral.

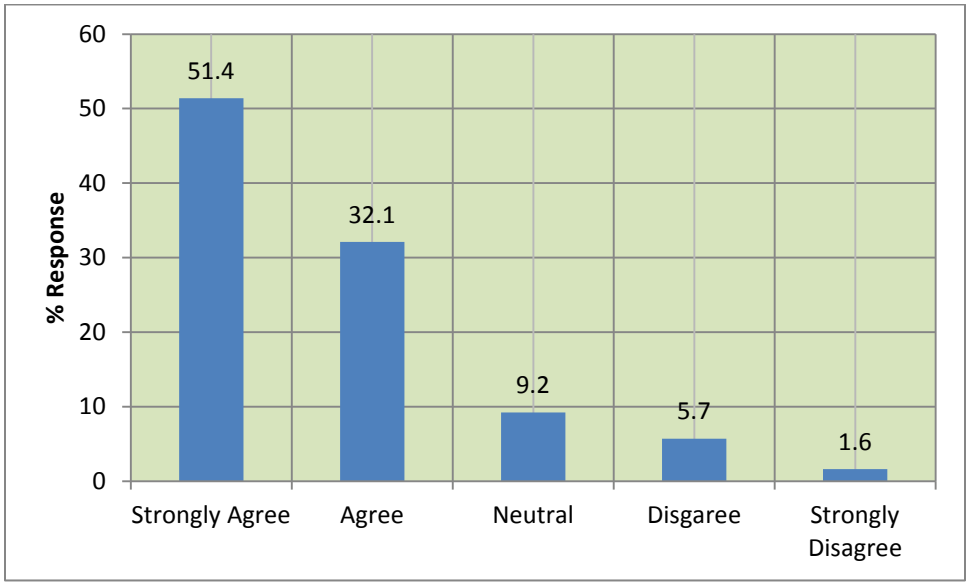

Figure 7-27: Diversity in working values and norms influenced the IS culture.

Interviewees agreed that there is diversity regarding the working values and norms of a hospital's employees. They argued that this is mainly due to the employees' different nationality and culture, educational backgrounds and attitudes. Each individual or group has its own values and norms towards information security. One of the interviewees stated the following:

> 'I have observed clearly that employees' working values and norms vary based on their national cultures, educational backgrounds and attitudes towards information security'
>
> (Interviewee A).

7.7.4 Employees' Multicultural Interactions

Figure 7.28 shows the responses towards the following statement: "Multicultural interactions in the hospital have influenced hospital employees' attitudes towards information security'. The vast majority, 57.8% (213 out of 368) of the respondents strongly agreed or agreed with the statement, and 33.7% (124 out of 368) strongly disagreed or disagreed with the statement. Only 8.4% (31 out of 368) remained neutral.

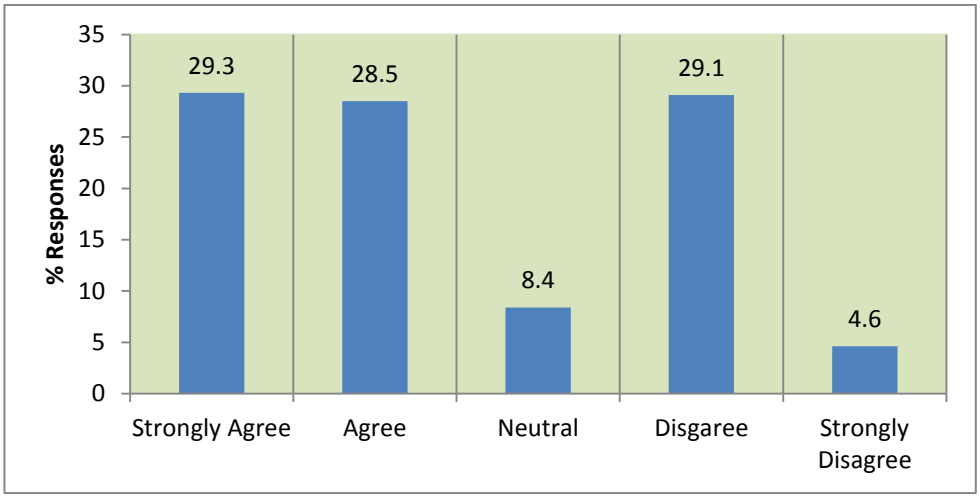

Figure 7-28: Diversity in working values and norms of the employees influenced the IS culture.

7.7.5 Employees Multicultural Background and Trust

Figure 7.29 shows the responses towards the following statement: "Employees multicultural backgrounds have influenced hospital employees' trust towards information security'. The vast majority, 72.9% (268 out of 368) of the respondents strongly agreed or agreed with the statement, and 17.4% (64 out of 368) strongly disagreed or disagreed with the statement, while only 9.8% (36 out of 368) remained neutral.

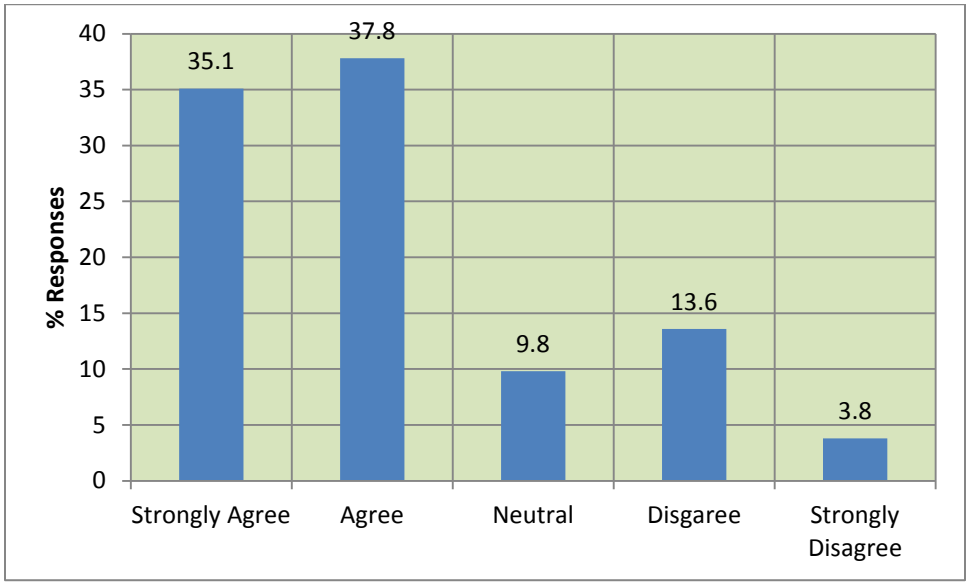

Figure 7-29: Hospital multicultural working environment influenced trust towards IS

Trust is explored as a critical dimension for the information security culture. It has been explored within several issues, which the interviewees discussed during the interviews. The interviewees believed that trust is critical for creating a positive information security culture in the hospitals. One of the employees explained,

> 'I have to see [that] trust is important for our relationship and how we interact within the hospital working environment, and no doubt, this has influence the IS culture of our hospital'
>
> (Interviewee D).

7.8 Role of Job Security and Job Satisfaction

This section presents an analysis role of job security and job satisfaction on information security in SA hospitals..

7.8.1 Role of Job Security

Job security has been explored by several interviewees as one of the main dimensions for individual behaviour in hospitals. This dimension explored and agreed by both Saudi and Non-saudi nationals working in the hospital. They agreed non-nationals are complying and behaving according to the hospitals rules and are very careful on disclosing any information to avoid any conflict with the management in order to extent their working contract, job security. One of the interviewees stated:

> 'It is clear for me that employees behave so well in the hospital to secure new, extension for their current employment contract. This clear for non-Saudi employees'
>
> (Interviewee K).

One of the interviewees explained the secured job, job for life, for the Saudi plays a major role in the employees' behaviour in the hospitals. The employee argued the job security has an impact on their behaviour, the interviewees stated:

> 'I can, personally, argued that Saudi job for life, secure job, has influenced their behaviour in the hospital particularly in disclosing information '
>
> (Interviewee E)

7.8.2 Role of Job Satisfaction on the Hospital IS

Job satisfaction explored as one of the main cultural dimensions that plays a role on the employees' behaviour and attitudes towards information security culture. The interviewees argued strongly that there is a strong link between the job satisfaction and the employees' behaviour. They argued satisfies and happy employees' enjoy their work and respect his or her role. The work enjoyment and respect of the role can lead to positive behaviour toward information and positive attitude towards job role tasks.

> 'Once the employees are happy and satisfied with his/her job role in the hospital, you can see and observe positive attitude and behaviour towards information security'
>
> (Interviewee E).

7.9 Summary

This chapter presented the evaluation process and data analysis collected to evaluate the research model. The evaluation analysis was based on analysing questionnaire and interviews of the second fieldwork visit. The main outcomes of this chapter will be used to enhance the research main outcomes discussion of the next chapter, chapter 8.

CHAPTER 8
DISCUSSION

The main objectives of this chapter are as follows:

- To discuss the current situation of SA NHS IS culture;
- To discuss the main drives for the IS culture policy;
- To discuss and evaluate the developed IS culture model; and
- To discuss the implementation of the SA IS culture policy.

Chapter 8 **: Discussion**

8.1 Introduction

The role and impact of a hospital's culture on information security has become one of the challenges for many organisations, and several examples are evident in the literature on this issue. This issue is relatively new and challenging in Saudi hospitals due to a lack of research in the field as well as the strong and distinctive culture of Saudi society. This research aims to develop an information security culture framework to help Saudi Arabia's help health service authority adopt progressive strategies on this issue. This chapter discusses the research's main findings based on the primary outcomes of the research. It focuses on the current situation of SA NHS IS culture, the drives for IS culture policy, discussions and evaluations of the IS culture framework, and how to make implementation practical when creating an IS culture policy.

8.2 Current Situation of SA NHS IS Culture

One of the main objectives of this research is to analyse the current situation of IS culture in Saudi Arabian hospitals. This is needed to help understand the extent of the challenge that this issue presents. In addition, this chapter discusses the current situation of IS cultures of Saudi Arabian hospitals based on the main outcomes of the literature review analysis as well as this research's primary outcomes.

8.2.1 Current IS Culture Practice

The literature survey and the data analysis of this research stressed the role and impact of hospital cultures on information security. Saudi hospitals are not aware of the importance and impact of a hospital's culture on protecting confidentiality, and integrity of information. In some cases, employees currently believe that revealing information to a third party is important, as doing so is part of their commitment to the hospital and to society. They believe that revealing information to a third party should be part of their norms and values within the organisation's activities. It is also has become normal practice in the hospital communication process to give medical reports and information to a third party, such as giving diagnostic results to a friend or relative without the patient's consent.

8.2.2 Current Drives for IS Culture Policy

The research identifies several drives for SA's National Health Service authority to introduce and implement clear strategies, to promote IS culture in its services. One of the drives is the current understanding and awareness of Saudi patients and employees about their rights regarding personal information (Al-dajani, 2011). Therefore, the working environment culture needs to be promoted through the demonstration of appropriate behaviour by employees to protect the individual's right to their information. Currently, there is no clear IS culture policy addressing this issue. Therefore, the authority needs to implement an action plan and develop a clear strategy for action.

The second drive is to avoid any legal conflict due to the expansion and effectiveness of legal firms in supporting patients' claims. This has become an important drive due to the fact that a large number of non-Saudi employees and companies operate in Saudi Arabia.

The other important factor is the image of the service. This needs to be high on the agenda of the authority due to the support and investment of the authority in the service. Any issue harming the image of the service may induce prejudice on the service's authority image and commitment towards providing appropriate healthcare services.

It also has been observed and explored in several interviews that employees leave their computer and/or monitor on while they go for a short break, leaving their desks. This leaves information and access to the information system exposed to any intruder. The other practice identified as norms amongst some of the employees, which includes providing their password to their colleagues.

Some hospitals are in the process of introducing and implementing electronic recording transmission of patient records as part of the hospital's operations, to improve the hospital, and the health care system's efficiency. However, from an information security culture point of view this is a challenge. This requires a change in the employees' behaviour towards information security. It requires awareness, knowledge and understanding of the electronic process to ensure that information cannot be transmitted and/or accessed by non-authorised persons.

8.3 Employees' Information Security Behaviour

At the individual level, the research developed an information security culture model to help identify main cultural dimensions that influence an individual's behaviour towards information security. This was achieved by testing several hypothesis related to these dimensions. These hypotheses are:

Hypothesis 1:

H1: Organization leadership positively related to the employee's attitude to health information security.

The research found that there is a positive relationship between the hospital leadership and information security culture within the hospital working environment. The qualitative data analysis supports this observed relationship. The research also indicated that Saudi leadership is impacted by Saudi Arabian national culture and is reflected in leadership management style, decision-making and behaviour towards the information security culture.

Hypothesis 2:

H2: Employees job satisfaction and job security is positively related to the employees' attitude towards information security.

Employees' job satisfaction has a positive correlation with the employees' attitudes towards information security behaviour. Job satisfaction in the hospital plays a major role in the employees' behaviour towards the information security culture. The qualitative data indicated that unsatisfied employees are less disciplined in complying with a positive information security culture. This is clearly evident amongst Saudis who are unsatisfied with their jobs and work in administration in the hospitals.

Hypothesis 3:

H3: Trust is positively related to employees' attitudes toward information security.

There is a positive relationship between employees' trust and their attitudes towards information security culture. Trust helps employees in complying with the hospital's procedures and regulations within the hospitals. Trust also promotes positive behaviour within the hospital.

Hypothesis 4:

H4: Saudi national culture is positively related to the employees' attitude towards information security.

The research confirmed that the Saudi national culture is a positively linked to the employees' attitude towards information security. The qualitative analysis indicated that the Saudi national culture has influenced information security culture of the hospitals and influenced the employees behaviour towards information security.

Hypothesis 5:

H5: Organisation communication is positively related to the employees' attitudes towards information security.

The research found that there is no link between the communication system and the information security culture within hospitals. It is important to note, however, that the qualitative analysis indicated that having a communication system helps in developing a positive information security culture.

Hypothesis 6:

H6: Employees' intention towards information security is positively related to the employees' attitudes towards information security.

The research confirmed a strong relationship between employees' intentions and their attitudes towards information security. Attitude plays a major role in forming employees' intentions to use information within the hospital. Having a positive attitude helps employees comply with information security rules and procedures, and improve the information security culture. On the other hand, having a negative attitude can lead to abusing information security—i.e., employees behave negatively where information security is concerned.

Hypothesis 7:

H7: Hospital multicultural backgrounds are positively related to information security.

The research indicated a positive relationship between Hospital multicultural backgrounds and employees information security behaviour. The qualitative data has also supported this hypothesis by explaining the main drives for the interaction between employees and the patients based on the cultural backgrounds.

8.4 Implementation of SA IS Culture Policy

The main purpose of developing an IS culture framework is to identify the influence of cultural dimensions on hospital information and to help Saudi authorities develop practical and effective IS culture policies. The main drive for this research is a lack of policy and strategy that recognises and considers the influence of culture on information security and the extents of not implementing appropriate policies and strategies. This research strongly argues for the importance and need to change the culture of organisations and make IS a part of their norms and values. This requires a clear IS culture policy and a clear strategy from the local hospital and Saudi Arabian authority. The policy and strategy need to be aimed at changing the employees' behaviour favourably towards information security. The policy and strategy should include the following, as outlined below.

8.4.1 Clear and Effective Employee IS Education Programmes

At the core of the health service authority is the need to focus on developing a clear statement in promoting and enhancing employees' information security awareness, knowledge and understanding. This helps in changing the employees' attitudes, perceptions and opinions to the hospital information. This change helps in altering employees' behaviour, according to behaviour theory. Education programmes should include training in information security. The programmes need to take in consideration three main elements of the effective learning process. The first is to keep in mind the trainee's learning style, ability, cultural background and job role. The second element is to select qualified and skilled trainers to facilitate the learning process. The third element is to provide an appropriate and convenient training environment. The training should be aimed at improving employees' attitudes and opinions favourably towards information security. One of the interviewees stressed the importance and the

role of employees' education programmes by stating the following: 'I do believe and understand that we need to establish clear and effective training programmes for our employees due to [the] lack of awareness and understanding of protecting patients' personal and medical [records] and employees' information'.

8.4.2 Promoting Social Interaction

One of the cultural dimensions identified is the trust amongst the employees themselves, and between employees and management. Therefore, health authority figures and hospital management need to adopt policies and strategies that aim to enhance trust by promoting encouraging and supporting interactions to help break down the barriers and establish understanding, respect and awareness of each other. These will help to develop trust amongst employees. This can be achieved by creating an appropriate environment for social interaction. This includes developing a strategy for creating appropriate and effective break and lunch time spaces as well as informal meetings and activities, such Christmas and Islamic festivals such as Eid activities. The strategy should be based on promoting encouraging and supporting social interactions for enhancing trust. On the other hand, the policy should be focused on establishing policies supporting social activities and contributing to social interaction costs, such as reducing healthy services operations cost

8.5 Barriers and Obstacles for Hospitals ISC in SA

This section discusses the main barriers and obstacles facing hospitals.

Employees' Resistance

One of the main barriers to implement information security policies is employee resistance. This is the mainly due to cultural dimensions that have been established within the hospitals. Employees need to change their daily behaviour values and norms in order to ensure effective policy implementation. Employees may resist making changes that are not within their norms and values. Employees' resistance towards change is the main challenge for health

authority figures. Therefore, authority figures need to take into consideration employees' resistance to changes that affect their daily routines.

Lack of Expertise and Knowledge in the ISC

Expertise and knowledge in the role of cultural dimensions in the ISC is critical to develop and implement a clear information security culture strategy and policy. One of the main problems in the Saudi authority is the lack of expertise and knowledge of ISC within the hospitals, and this has impacted on protecting hospital information. The hospitals lack individuals with appropriate ISC knowledge to help with developing and promoting an information security culture. One of the hospitals' employees explored this issue and stated the following: 'I would like to inform you in simple language that we, as a hospital, lack [the] expertise and knowledge [of what is needed in an] information security culture. As one of this hospital's managers, this is the first time [that this has] come to my attention—[that is], the need to consider this cultural issue'.

The above statement has been commonly expressed in several interviews, which indicates that the hospitals fall short in having appropriate expertise and knowledge available to develop and promote an effective information security culture. It is clear that the hospitals lack an understanding of the importance of cultural dimensions on the employees' behaviours. Knowledge and expertise can help in developing appropriate policies and strategies for the hospital, and also in sharing this knowledge with others. It can also help in developing training for other information security issues.

Authority Opinions and Attitudes

SA health services are centralised and managed by a central authority. The health authority is the decision-making group, and there is little for the hospital to argue with or to say in the decision-making process and in the policies enacted by the health authority. Therefore, the health authority's opinions and attitudes regarding information security, in general, and the information security culture, in particular, has a great influence on the hospital's information security practices. It is clear from this research that the authority lacks the right attitudes regarding information security culture. This has been identified in their management approach. In the first approach, there is no policy or strategy found in any Saudi hospitals regarding the development of an information security culture. The current policy is mainly technology-based and requires a username and password to access information within the hospitals. From the authority's perspective, this should be enough to protect private information. The second approach is found in the following interviewee's statement. It reveals the main barrier to establishing a positive information security culture and investing in employees' awareness and knowledge about the necessity for protecting a hospital's information: 'I have written several times and mentioned in several meetings with the authority about the importance of investing in the employees' knowledge and understanding of information security. I have also suggested to give scholarships and invite speakers on the issues, BUT the authority never responded' (Interviewee D).

Hospital Priority

The hospital's information security culture is relatively new for hospital management and employees. There is a lack of awareness of the impact of the hospital's culture on information protection. One of the main reasons for this, as identified by hospital management are the hospital's own priorities. As one of the interviewee says, 'I do understand the point of view you are trying to stress. I think that the health services priority is building the medical staff and infrastructure of the health service. Possibly in [the] near future, the information security culture may take [on] another dimension [of importance]'.

Lack of Awareness and Understanding of the Patient's Rights and Citizen's Privacy

One of the main challenges in promoting and enhancing information security in Saudi hospitals is the lack of awareness and understanding among the hospital staff and patients of patient's rights and privacy. This has influenced the staff members' behaviour in managing and handling hospital information. Misuse of information has become part of the hospital culture. The staff lacks an understanding of the importance and the right of the individual to privacy, as well as the fact that his or her personal data and information should also be kept confidential, and the information must not disclosed to a third party without the patient's permission. National culture plays a role in the staff members' behaviours and attitudes.

Lack of National Information Security and Privacy Legislations

This research identified that there is a lack of clear national information security in the Kingdom with respect to health services information. The research also identified that there is a lack of national privacy legislation to protect individuals' privacy. At the national level this contributes to the lack of policy and procedures to protect information in the Kingdom hospitals. It can also be argued that the lack of national information and privacy legislations at the national level have also contributed to individual employees' behaviour towards information security.

8.6 Needs for Changes in SA Hospital Information Security Culture

In order for Saudi health services to have effective information security, they need to be able to cope with changes in the health service, both internally with the use of technology, and externally in considering economic and political environments. This research is argues that the changes need to address three main elements of the health service' strategic planning and operational activities.

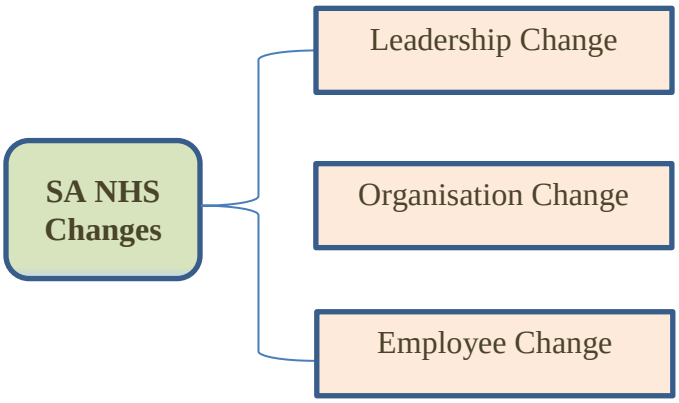

Figure 8-1: SA national health services changes

Organisation Change

One of the changes is organisational, or hospital change.. The hospital should be able to change to ensure that it can build a positive information security culture. The organisation should have the capability to change its strategies, policies, systems and processes to help in building its structure. The changes should also include changes in leadership and senior management's attitudes and opinions towards information security. The organisation needs to have the capability to cope with the possibility of some employees resisting change.

Change Organisation in Leadership and Authority Members' Attitudes and Opinions toward IS

The SA National Health Service is mainly public and centralised, and decision-making and strategic planning are made by authorities and senior management, with no or little contribution from others in the decision-making process. Therefore, the current authority's opinions and attitudes towards the information security culture need to be changed in order to help with investing and decision-making to build a positive information security culture. This can be achieved by providing authorities with evidence, such as the outcome of this research and educational programmes through seminars and formal and informal meetings.

Change in Employees

The role and impact of health services employees' behaviour on protecting and ensuring information security is quite evident from this research's main findings as well as the literature. The use of technology is not enough without appropriate employees' behaviours towards information. This research identified several dimensions that contribute to employees' attitudes as well as the role of attitude on actual employees' behaviours. Therefore, the main task of the authority is to change the employees' attitudes towards information security.

8.7 Summary

This chapter discussed and presented the current situation of the SA NHS culture. This includes the current situation of SA NHS IS culture practice and the current drives for adopting an appropriate information security culture policy. Barriers and obstacles for hospitals ISC in SA were also discussed and presented. The chapter also discussed the current drives for information security culture policy. The chapter closes with a discussion on the need for changes in SA hospital information security culture.

CHAPTER 9
CONCLUSIONS, RECOMMENDATIONS AND SUGGESTIONS FOR FUTURE WORK

Chapter 9 Objectives

The main objectives of this chapter are as follows:

- To summarise the research main outcomes;
- To present the research main contributions;
- To provide practical recommendations to the Saudi Arabian health authority;
- To provide suggestions for future work based on the main findings of the research.

Chapter 9 : Conclusions, Recommendations and Suggestions for Future Work

9.1 Introduction

SA health services have developed sharply in recent years due to investment by the authorities to improve health services. It is also important to stress the development and changes in the services due to increased awareness of citizens concerning their right to receive appropriate health care service, and their rights to their own medical information. This is mainly due to a need to improve the education system and interaction with other societies, as the Saudi society has become a more open society in recent decades. It is also important to stress that the authorities are also in the process of introducing and implementing electronic recording, particularly regarding patients' electronic records.

One of the main challenges in the SA health care services is protecting the patient's medical records, while changes and expansion in health care operations and recording processes develop. The vast majority of research on information security protection in SA neglects the role of the hospital's culture on information security. This research's main focus is on the role of humans in protecting information security by identifying the main cultural dimensions and sub-dimensions of employees' attitudes to information security. The aim is to develop an information security culture framework model that can help in developing and implementing an appropriate information security culture. The research identified the main drives for the IS culture framework model in Saudi Arabia. The research also carried out a critical review of the related literature and collected data and information from three main hospitals in Saudi Arabia to

develop an IS framework model. A second survey was carried out to evaluate and test the developed IS security culture model.

This chapter presents the main conclusions of the research's primary findings and provides practical recommendations. The chapter closes with suggestions for future research in the information security culture in Saudi Arabia.

9.2 Conclusions

The main contribution of this research can be described in three main points. The first is in analysing and evaluating current hospitals' IS cultures. The second involves analysing and identifying the main IS cultural dimensions that influence a hospital's IS culture. The third entails developing an IS culture framework model based on the employees' attitudes and behaviour towards information security. This section presents the main conclusions of the research.

- The research identified that human behaviour towards medical information in SA is one of the main threats to information security and one of the main challenges to SA health authorities. The SA health authority needs to take into consideration the human element of its operation as part of its strategy to protect the hospital's information.
- The current situation of SA hospitals' IS cultures is inadequate for protecting medical information due the current values and norms towards information security. This is mainly due to the employees' attitudes towards IS because of its set of dimensions and sub-dimensional culture.
- The research developed and evaluated an IS culture framework model for SA hospitals. The model is based on human behaviour theory, where the individual's attitude is the key element of the individual's intention to behave as well as of his or her actual behaviour. The research identified six cultural dimensions: Saudi national culture, Saudi health service leadership, employees' trust, technology, multicultural interactions and employees' job roles. The research also identified a set of cultural sub-dimensions. These include working values and norms, tribe values and norms, attitudes towards women, power sharing, vision, social interaction, respect and understanding,

hospital intranet, hospital employees' language(s) used, multi-national culture, communication system, employees' job satisfaction and job security. These dimensions and sub-dimensions contribute to the employees' attitudes towards IS. However, the weight of each of these dimensions and sub-dimensions varies. The research identified that Saudi national culture and employees' job roles are the main issues affecting employees' attitudes, and conversely technology is the least important issue in this regard.

The main outcomes of the research on the research hypothesis

- Hypothesis 1: There is a positive relationship between organisation leadership and employees' attitudes towards health information security.
- Hypothesis 2: There is a positive relationship between employees' job satisfaction and job security and their attitude towards information security.
- Hypothesis 3: There is a positive relationship between trust and the employees' attitudes towards information security.
- Hypothesis 4: There is a positive link between an organisation's information security policy and the employees' attitude towards information security.
- Hypothesis 5: There is no link between organisation communication and employees' attitudes towards information security.
- Hypothesis 6: Employees' intentions regarding information security are related to the employees' attitudes towards information security.
- Hypothesis 7: Employees' intentions are related to their actual behaviour in relation to information security.

9.3 Recommendations

The research identified as important, a need for change in the information security culture within Saudi Arabian hospitals. It shows the human behaviour part of information security is critical to protect patients' medical information. The following are the main practical recommendations that need to be considered by the Saudi health service authority to promote and enhance an information security culture.

9.3.1 Developing IS Culture Policy

The lack of an appropriate information security culture policy in Saudi hospitals stresses the need to develop such a policy. The policy should take into consideration the dimensions and sub-dimensions that are culturally identified as part of the developed model of the research. The policy should also aim to promote and enhance the information security culture within the organisation.

9.3.2 Hospital Employees Education in IS culture

One of the key elements of information security is the employees' behaviour towards the information security culture. Therefore, it is highly recommended to develop employees' information security culture educational programmes to enhance and improve employees' knowledge, understanding and awareness of information security. The educational programmes need to take into consideration three main factors. The first is the employees' learning styles. The educational programmes need to be designed specifically based on the trainees' learning styles. The second factor is the trainer and training approach. This factor emphasises the importance of ensuring that the training programme be delivered by highly skilled and competent trainers, who provide training that is appropriate to the trainees' abilities.

The third factor is providing an appropriate learning environment to help facilitate the learning process.

9.3.3 Developing IS Culture Environment

The research identified several dimensions and sub-dimensions that influence the information culture environment. One of these dimensions is trust amongst employees and between the management and employees. The research recommends improving trust through promoting employees' interactions amongst themselves through formal and informal events. This may lead to greater instances of social interaction. This can be achieved by creating an appropriate environment for interaction, and establishing an efficient and effective communication system, such as the hospital intranet, to support the interaction. Improving the working environment, sharing power with employees and ensuring job satisfaction are all steps that need to be taken into consideration as part of the hospital's improving the hospital IS culture strategy.

9.4 Limitations of the Research

One of the limitations that can't be easily implementation even we know changes are needed to improve the hospital information security culture is the culture factor, employees individual culture and the hospital working culture. Change in culture required long and careful processes and strategy.

9.5 Suggestions for Future Work

The information security culture in SA health services requires further investigation and analysis to enhance the current research's main findings. This research suggests the following areas for further future research.

Implantable Suggestions

- There is a need to evaluate and develop the information security model further by involving private hospitals to make the model more generic and to help the health service authority develop an effective information security policy.
- One of the main areas related to developing an information security culture is changes in management styles, structure and communication systems. There is a need for research focusing on hospital management capabilities and strategies in developing an effective information security culture.
- There is a need for research on information security culture policies. This includes establishing appropriate rules and regulations for the information security culture. At this stage, SA health services lack an information security culture.
- There is a need for research on national information security culture policies.

Other Recommendations

- One area identified as in need of further research is the information privacy culture within Saudi health services. Currently, there is a lack of research and understanding of information privacy culture.
- There is a need for research that focuses on SA health services employees' behaviour towards information security.

- SA health services have established strategies for implementing electronic patient recording throughout their services. Therefore, there is a need for research on the electronic security culture within the SA hospitals.
- There is a need for research to clarify the patient's information ownership with SA hospitals due to the conflict between the patient's rights and organisation's rights.

References

Adams, A., et al. (2005). Bridging the gap between organizational and user perspectives of security in the clinical domain. *International Journal of Human-Computer Studies*,*63*(1-2), 175–202.

Adesina, A., Agbele, K., Februarie, R, Abidoye, A., & Nyongesa, H. (2011). Ensuring the security and privacy of information in mobile health-care communication systems. *South Africa Science Journal, 107*(9/10), 26–32.

Ackerman, M. (2004). Privacy in pervasive environments: Next generation labelling protocols. *Personal and Ubiquitous Computing*, 8(6), 430–439.

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behaviour*. Englewood Cliffs, NJ: Prentice Hall.

Algie, J. (1975). *Social values, objectives and action*. NJ: Prentice Hall.

Appadurai, A. (1990). Disjuncture and difference in the global cultural economy. In Featherstone, M. (Ed.), *Global culture: Nationalism, globalisation and modernity*. London: Sage. In Craig, C. and Douglas, S. 2006. Beyond national culture: Implications of cultural dynamics for consumer research. *International Marketing Review*, *23*(3), 322–342.

Ashkanasy, N. M., Broadfoot, L. E., & Falkus, S. (2000). Questionnaire measures of organizational culture. In N. M. Ashkanasy, C. P. M. Wilderom, & M. F. Peterson (Eds.), *Handbook of organizational culture and climate*. Thousand Oaks, CA: Sage Publications.

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *Journal of Strategic Information Systems, 11*(3/4), 245–270.

Beldad, A., de Jong, M., & Steehouder, M. (2011). A comprehensive theoretical framework for personal information-related behaviours on the Internet. *The Information Society, 27*(issue), 220–232.

Briggle, A., & Mitcham, C. (2009). From the philosophy of information to the philosophy of information culture. *The Information Society, 25*(1), 169–174.

Burke W.W. (2002) *Organization Change: Theory and Practice*. Sage, London.

Camp, L. J. (1999). Web security and privacy: An American perspective. *Information Society*, 15(4), 249–256.

Campbell, J. and Goritz, A., (2014) Culture Corrupts! A Qualitative Study of Organizational Culture in Corrupt Organizations. Journal of Business Ethics, 120(3), *Journal of Business Ethics 1*, pp 291-311

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security at the workplace: Linking information security climate to compliant behaviour. *Journal of Information Privacy and Security*, *1*(3), 18–42.

Chang, S., and Lin, C. (2007). Exploring organisational culture for information security management. *Industrial Management & Data Systems, 107*(3), 438-458.

Chen, Y., Cheng, B., Chen, H., Lin, C., Liao, G. B., & Hsu, S. (2012). A privacy-preserved analytical method for eHealth database with minimized information loss. *Journal of Biomedicine and Biotechnology*, 2(4), pp. 213-219.

Clark, J. (2008). How secure is your hospital's front door? *Information Security Journal: A Global Perspective*, *17*(1), 201–202.

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. *Communications of the ACM*, *42*(2), 60–67.

Clough, P., & Nutbrown, C. (2007). *A student's guide to methodology: Justifying enquiry.* 2nd ed. London: Sage.

Craig, C., & Douglas, S. (2006). Beyond national culture: Implications of cultural dynamics for consumer research. *International Marketing Review*, *23*(3), 322–342.

Creswell, J. (2003). *Research design: Qualitative, quantitative, and mixed methods approaches.* 2nd ed. London: Sage Publications.

Culnan, M., & Armstrong, P. (1999). Information privacy concerns, procedural fairness and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104–115.

Currie G. & Lockett A. (2007) A critique of transformational leadership: moral, professional and contingent dimensions of leadership within public services organizations. *Human Relations* 60, 341–370.

Da Veiga, A., and Eloff, J. (2010). A framework and assessment instrument for information security culture. *Computer & Security, 29*, 196-207.

Deal, T., & Kenny, A. (1982). *Corporate culture: The rites and rituals of corporate life.* Reading, MA: Addison-Wesley.

Deng, M., Wuyts, K., Scandariato, R., Preneel, B., & Wouter Joosen, W. (2011). A privacy threat analysis framework: Supporting the elicitation and fulfilment of privacy requirements. *Requirements Engineering*, *16*(1), 3–32.

Desai, T. (2011). Initiative to change ward culture results in better patient care. *Nursing Management*, *8*(4), pp. 14-29.

Dickson, C., and Smith, M., (2013). Time for change in community nursing? A critique of the implementation of the Review of Nursing in the Community across NHS Scotland. *Journal of Nursing Management*, 21, 339–350.

Eastlick, M. A., Lotz, S. L., & Warrington, P. (2006). Understanding online B-to-C relationships: An integrated model of privacy concerns, trust, and commitment. *Journal of Business Research*, *59*(8), 877–886.

Eloff, J. (2003). Information security management-Anew Paradigm, *Proceedings of SAICSIT* 2003, 130 –136.

Fetter, M. (2009). Personal health records: Protecting behavioural health consumers' rights. *Issues in Mental Health Nursing*, *30*, 720–722.

Engelen, A., Flatten, T., Thalmann, J., and Brettel, M., (2013). The Effect of Organizational Culture on Entrepreneurial Orientation: A Comparison between Germany and Thailand., 52(4), pp 732-752.

Gerber, M., and Solms, R. (2008). Information security requirements - Interpreting the legal aspects, *Computers & Security*, 27(5-6), 124-135.

Gregory, N. S., Kathleen, L. M., & Charles, R. G. (2007). Organizational culture, critical success factors, and the reduction of hospital errors. *International Journal of Production Economics*, *106*(2), 368–392.

Gunter, T. D., & Terry, N. P. (2005). The emergence of national electronic health record architectures in the United States and Australia: Models, costs, and questions. *Journal of Medical Internet Research*, 7(1), 125-132.

Haralambos, M., Holborn, M., & Heald, R. (2004). *Sociology: Themes and perspective.* 6th ed. London: Harper Collins Publishers Limited.

Harvey, F. (1997). National cultural differences in theory and practice: Evaluating Hofstede's national cultural framework. *Information Technology & People*, *10*(2), 132–146.

Hatch MJ (2002) *Organization Theory: modern symbolic and postmodern perspectives*. Oxford Books: Oxford.

Henderson A., Briggs, J., Schoonbeek, S., & Paterson, K. (2011). A framework to develop a clinical learning culture in health facilities: Ideas from the literature. *International Nursing Review*, *1*(2), 196–202.

Herath, T., & Rao, H. (2009). Encouraging information security behaviours in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*, 154–165.

Hofstede, G. (1980). *Culture's consequences: International differences in work-related values.* London: Sage Publications.

Hofstede, G. (1997). *Cultures and organisations: Software of the mind.* New York: McGraw-Hill

Hofstede, G. (2001). *Culture's consequences: Comparing values, behaviours, institutions, and organisations across nations.* London: Sage Publications.

Hopkins, A. (2006). Studying organizational cultures and their effects on safety. *Safety Science*, 44, 875–889.

Huang, D., Rau, P. P., & Salvendy, G. (2007). A survey of factors influencing people's perception of information security. In J. Jacko (Ed.), *Human-Computer Interaction, Part IV*. Heidelberg: Springer.

Huang, L.C., Chu, H.C., Lien, C.Y., Hsiao, C.H. and Kao, T. (2009) "Privacy preservation and information security protection for patients' portable electronic health records", *Computers in Biology and Medicine*, 39(9), 743-750

Joiner, T. (2001). The influence of national culture and organizational culture alignment on job stress and performance: Evidence from Greece. *Journal of Managerial Psychology*, *16*(30), 229–242.

Kahler, E. G. (1968). Culture and evolution. In M. F. Montagu (ed.), *Culture: Man's adaptive dimension.* London: Oxford University Press.

Kidd, W. (2002). *Culture and identity*. New York: Palgrave.

Kritzinger, E., and Smith, E. (2008). Information Security Management: An Information Security Retrieval and Awareness model for industry. *Computer & Security, 27,* 224-231

Kruger, H. A. & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security*, *25*, 289-296.

Lacohee, H., Phippen, A. D., & Furnell, S. M. (2006). Risk and restitution: Assessing how users establish online trust. *Computers and Security*, *25*, 486-493.

LaRose, R., & Rifon, N. (2006). Your privacy is assured—of being disturbed: Comparing web sites with and without privacy seals. *New Media and Society*, *8*(6), 1009–1029.

Leslie, G. (1979). *The family and social context.* New York: Oxford University Press.

Lim, J., Chang, S., Maynard, S., & Ahmad, A. (2009). Exploring the relationship between organizational culture and information security culture. *Proceedings of the 7th Australian Information Security Management Conference.* Location: Publisher.

Malhotra, N., Kim, S., and Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355.

Martin J., (2002). *Organizational Culture: mapping the terrain*. Sage Publications: London.

McBride, M. (2008). Google health: *Birth of a giant. Health Management Technology*, *29*, 8–10.

McBurney, D., and White, T. (2004). *Research methods*. Thomson: Australia.

McGuire, J., Rhodes, G., and Palus, C, (2008) . Transforming Your Leadership Culture, *LIA*, 27(6)

McIlwraith, A. (2006). *Information Security and Employee Behaviour*. Aldershot, Hampshire, UK: Gower.

Morden, T. (1999). Models of national culture— a management review. *Cross Cultural Management*, *6*(1), 10–4.

Morgan, D. (1985). *The family, politics and social theory.* London: Routledge & Kegan Paul.

Muhaya, F., Hadi, F., and Minhas, A. (2012). On the development of comprehensive information security policies for organizations. *International Journal of Academic Research*, *4*(1), 16–22.

Neuman, W. L. (2006). *Social Research Methods: Qualitative and Quantitative Approaches*. Boston: Pearson.

Oakely, A. (1981). *Subject women.* Oxford: Martin Robertson.

Pallant, J. (2005). *SPSS Survival Manual: A Step by Step Guide to Data Analysis using SPSS for Windows (Version 12)*. Berkshire: Open University Press.

Patnaik, J., (2011). Role of work culture in improving organisation health. *Amity Journal of Applying Psychology*. 2(1), 40-48.

Pavlou, P. (2011). State of the information privacy literature: Where are we now and where should we go? *MIS Quarterly*, 35(4), 977–988.

Pearcey, P. (2007). Tasks and routines in 21st century nursing: Student nurses' perceptions. *British Journal of Nursing*, *16*(5), 296–300.

Pieters, W. (2011). The (social) construction of information security. *The Information Society*, *27*, 326–335.

Rainer, R., & Marshall, T. (2007). Do information security professionals and business managers view information security issues differently? *Information Systems Security*, *16*, 100–108.

Reed, B. (2007). Implementing information lifecycle security (ILS). *Information Systems Security, 16*, 177–181.

Robbins S.P. & Judge T.A. (2008*) Essentials of Organizational Behaviour*, 9th edn. Pearson Prentice Hall, New Jersey.

Rotvold, G. (2008). How to create a security culture in your organization? *The Information Management Journal, 1*(4), 33–38.

Rubinstein, I. (2011). Regulating privacy by design. *Princeton's Centre for Information Technology Policy, and the Privacy Law Scholars*, 1410–1453.

Ruighaver, A. B., Maynard, S. B., & Chang, Initial. (2007). Organisational security culture: Extending the end-user perspective. *Computers and Security*, *26*, 56–62.

Schein, E. H. (1992). *Organisational culture and leadership*. San Francisco: Jossey-Bass Publishers.

Schein, E. (2004). *Organizational Culture and Leadership*, Third edition, San Francisco: Jossey-Bass, CA.

Schein E. (2010). *Organisational Culture and Leadership*, San Francisco: Jossey-Bass, , CA.

Schultz, E. (2005). The human factor in security. *Computers and Security*, *24*, 425–426.

Schmiedel, T., Brocker, J., and Recker, J., (2014). Development and validation of an instrument to measure organizational cultures' support of Business Process Management, *Information Management*, 51(1), 43-56.

Sekaran, U., and Sekaran, U. (1992). Research methods for business: A skill building approach. 2nd ed. New York: Publisher.

Siponen, M., and Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *SIGMIS Database*, *38*(1), 60–80.

Skinner, G., Han, S., and Chang, E. (2006). An information privacy taxonomy for collaborative environments. *Information Management & Computer Security*, *14*(4), 382–394.

Skyttner, L. (1996). *General systems theory: An introduction*. London: McMillan Press Ltd.

Smith, H. J., Milberg, S. J., and Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, *20*(2), 167–196.

Smith, H. J., Dinev, T., and Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989–1015.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review*, 154(3), 477–564.

Spiers J (2003). *Patients, Power and Responsibility*. Radcliffe Medical Press: Oxford.

Stedham, Y., & Yamamura, J. (2004). Measuring national culture: Does gender matter? *Women in Management Review*, *19*(5), 233–243.

Sweeny, I, & Hardaker, M. (1994). The importance of organizational and national culture. *European Business Review, 94*(5), 3–14.

Thomson, K., & von Solms, R. (2005). Information security obedience: A definition. *Computers & Security, 24*(1), 69–75.

Van Niekerk, J., von Solms, R., (2010). Information Security culture: A management perspective. *Computers & Security*, 29, 476-486.

Van Niekerk, J., & Von Solms, R. (2005). An holistic framework for the fostering of an information security sub-culture in organizations. *Information Security South Africa (ISSA), Johannesburg, South Africa*.

Verbeeten, F. H. M. (2008), Performance management practices in public sector organizations: Impact on performance. Accounting, *Auditing & Accountability Journal*, 21(3), 427-454.

Vielba, C. (1995). Teaching managers about culture: Why mangers find formal models of organizational culture difficult to comprehend and work with. *Journal of European Training*, *19*(1), 4–9.

Walsham, G. (2006). Doing Interpretive Research. *European Journal of Information Systems*, 15(3), 320-330.

Wang, S., Beatty, S. E., and Foxx, W. (2004). Signalling the trustworthiness of small online retailers. *Journal of Interactive Marketing*, *18*(1), 53–69.

Worthington, F. (2004). Management, change and culture in the NHS: rhetoric and reality. *Clinician in Management*, **12**, 55–67.

Xu, H., Teo, H., Tan, B., & Agarwal, R. (2010). The role of push-pull technology in privacy calculus: The case of location-based services. *Journal of Management Information Systems, 26*(3), 137–176.

Watson, T. (2006). *Organising and Managing Work*, UK: Pearson Education Limited.

Williams, P. (2013). Does the PCEHR mean a new paradigm for information security? Implications for health information management. *Health Information Management Journal*, 42(2), 31–34.

Workman, M., Bommer, W., & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behaviour, 1*(2), 38-44.

Young, C. (2007) Organization Culture Change: The Bottom Line of Diversity, *the Changing Currency of Diversity*, 15(1), 26-32.

Zalami, A. (2005) *Alignment of Organisational Cultures in the Public and Private Sectors*, Presentation given at Excellence in Public Service, Amman, Jordan in September 2005.

Appendix A: Questionnaire: Identifying the problem

De Montfort University

Questionnaire: Identifying the problem

Culture dimensions of information systems security in Saudi Arabia National Health Services

S. Al-omran

July 2011

Dear Participants,

I am currently pursuing PhD research at University of De Montfort, United Kingdom. A key aim of my research aim is to investigate and analyse information security culture in Saudi Arabia National Health Services. I would like your kind contribution in the research process by completing the attached questionnaire. The data derived from the questionnaires will be used in analysing and recommendations for Kuwaiti Saudi Arabia National Health service and I would also like to stress that all responses will be treated confidentially and will be anonymous. Please do not hesitate to contact me if you need any clarification or question.

Salah Al-omran, BA, MA
Computer Science
De Montfort University,
Leicester,
UK
saleh.alomran@hotmail.com

Please tick √ in the box for your appropriate answer

Section A: Personal Details

Q1. Please specify your hospital

1	King Faisal Specialist Hospital and Research centre	☐	☐
2	King Fahad Medical City Hospital	☐	
3	Specialised Medical Centre Hospital	☐	

Q2. Please specify gender

1	Male	☐	☐
2	Female	☐	

Q3. Please specify nationality

1	Saudi national	☐	☐
2	Non Saudi	☐	

Q4. Please specify which discipline matches your job-role closest

1	Consultant	☐	☐
2	Resident	☐	
3	Medical students	☐	
4	Nurse	☐	
6	Medical technician	☐	
6	Manager	☐	
7	Administrator	☐	
8	Other (Specify the discipline) ……..	☐	

Q5. Please specify your experience in the organisation

1	Less than 5 years	☐	☐
2	5-10 years	☐	
3	11-15 years	☐	
4	16-20 years	☐	
5	21-25 years	☐	
6	Over 25 years	☐	

Section B: Leadership Style in the Organisation Management

		Strongly Agree	**Agree**	**Neutral**	**Disagree**	**Strongly Disagree**
Q1	Hospital leadership creates an information security environment where the employees take ownership	☐	☐	☐	☐	☐

of their tasks

Q2	Hospital asks employees for their vision of where they see information security going and then use their vision where appropriate.	☐	☐	☐	☐	☐
Q3	Hospital delegates tasks in order to implement a new procedure or process in the in hospital.	☐	☐	☐	☐	☐
Q4	Hospital leadership like to share information security power with employees	☐	☐	☐	☐	☐
Q5	Hospital takes group vote on what to do next in the hospital information security policy.	☐	☐	☐	☐	☐
Q6	National culture has influenced the leadership style in the hospital information security culture.	☐	☐	☐	☐	☐
Q7	National culture values and norms have a role on the leadership information security decision making process.	☐	☐	☐	☐	☐

Section C: Hospital Culture

		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Q1	Change in the hospital information security policy from traditional to electronic is a challenge.	☐	☐	☐	☐	☐
Q2	The hospital uses effective information security policy to protect Electronic Patient Record.	☐	☐	☐	☐	☐
Q3	Hospital employees are aware of the importance of health information security.	☐	☐	☐	☐	☐
Q4	Hospital employees have positive norms and values toward information security	☐	☐	☐	☐	☐
Q5	The hospital has appropriate information security environment.	☐	☐	☐	☐	☐
Q6	Trust among the hospital employees is important for the hospital information security.	☐	☐	☐	☐	☐
Q7	There is lack of trust among the employees due to lack of effective hospital culture.	☐	☐	☐	☐	☐
Q8	Trust between the employees and management is important for information security.	☐	☐	☐	☐	☐
Q9	There is a lack of trust between the employee and technology regarding information security.	☐	☐	☐	☐	☐
Q10	Shift from traditional medical recording to electronic record represent a threat to job security.	☐	☐	☐	☐	☐
Q11	Shift from traditional medical record to electronic record faces resistance from the employee.	☐	☐	☐	☐	☐

Section D: Hospital information security policy culture

		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Q1	Hospital has a clear information security.	☐	☐	☐	☐	☐
Q2	Hospital employees' aware of the current information security policy.	☐	☐	☐	☐	☐
Q3	Hospital employees are aware of the importance of health information security.	☐	☐	☐	☐	☐
Q4	Employees have a negative attitude towards information security.	☐	☐	☐	☐	☐
Q5	The employees never were in a training courses regarding information security.	☐	☐	☐	☐	☐
Q6	Employees do not respect the current information security.	☐	☐	☐	☐	☐
Q7	Employees resist shift from traditional to electronic information security policy.	☐	☐	☐	☐	☐
Q8	The current information security does not reflect the current use of electronic record.	☐	☐	☐	☐	☐
Q9	There is a lack of trust between the employee and technology regarding information security.	☐	☐	☐	☐	☐
Q10	The current policy does not take patient right into consideration	☐	☐	☐	☐	☐

Section E: Role of National Culture

		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Q1	Saudi national culture has influenced the hospital information security culture.	☐	☐	☐	☐	☐
Q2	Social division of the groups within the hospital plays a role in the hospital information security.	☐	☐	☐	☐	☐
Q3	Individual values and norms have an impact on the hospital information security.	☐	☐	☐	☐	☐
Q4	Employees' national culture backgrounds created cultural groups within the organisation effected the organisation management.	☐	☐	☐	☐	☐
Q5	Saudi national culture has influenced the influenced hospital management information security policy.	☐	☐	☐	☐	☐
Q6	Different languages used in the hospital are barrier for the hospital information security.	☐	☐	☐	☐	☐
Q7	National culture has a positive role in the employees' social interaction regarding information security.	☐	☐	☐	☐	☐
Q7	Employees social interaction has helped to improve information security	☐	☐	☐	☐	☐

Appendix B: Interview Design-Identifying the problem

De Montfort University

Interviews: Identifying the problem

Culture dimensions of information systems security in Saudi Arabia National Health Services

S. Al-omran

July 2011

Section A: information security policy

Q1: Does your hospital have information security policy?

……

……

……

……

……

……

Q2: How the hospital employees values information security?

……

……

……

……

……

……

Q3: What are the main culture-related barriers to information security policy at your hospital?

……

……

……

……

……

……

Section B: Role of hospital culture on Organisation Management

Q1: What is in the current hospital information security culture and what are your perceptions for promoting working vales and norms at your hospital?

……

……

……

……

……

……

Q2: What is the role of technology on promoting organisation information security culture at your hospital?

……

……

……

……

……

……

Q3: Can you explain information security instruction in your hospital?

……

……

……

……

……

……

……

Section C: National Culture and Organisation Management

Q1: what is the role and impact of Saudi national culture on information security culture at your organisation?

……

……

……

……

……

……

……

Q2: Your organisation employees come from different national culture, what is the impact of such diversity in the employees' cultural background on your information security culture?

……

……

……

……

……

……

……

Q3: Is the language is barrier between the employees and the management and the employees in the information security?

……

……

……

……

……

……

Many thanks for completing the questionnaire

Appendix C: Information Security culture model evaluation: Questionnaire design

De Montfort University

Information Security Model Evaluation Questionnaire

Culture dimensions of information systems security in Saudi Arabia National Health Services

S. Al-umaran

March 2013

Dear Participants,

I am currently pursuing PhD research at University of De Montfort, United Kingdom. A key aim of my research aim is to investigate and analyse information security culture in Saudi Arabia National Health service. I would like your kind contribution in the research process by completing the attached questionnaire. The data derived from the questionnaires will be used in evaluating and testing role of culture on information security model in Saudi Arabia National Health service and I would also like to stress that all responses will be treated confidentially and will be anonymous. Please do not hesitate to contact me if you need any clarification or question.

Saleh Al-umaran, BA, MA
Computer Science
De Montfort University,
Bede Island, Leicester, England
saleh.alomran@hotmail.com
Tel: (+966) 555454156

Please tick (√) in the box for your appropriate answer

Section A: Personal Details

Q1. Please specify your hospital

1	King Faisal Specialist Hospital and Research centre	☐	☐
2	King Fahad Medical City	☐	
3	Specialised Medical Centre Hospital	☐	

Q2. Please specify gender

1	Male	☐	☐
2	Female	☐	

Q3. Please specify your nationality

1	Saudi national	☐	☐
2	Non Saudi	☐	

Q4. Please specify which of the following matches your job-role closest

1	Consultant	☐	☐
2	Resident	☐	
3	Medical students	☐	
4	Nurse	☐	
6	Medical technician	☐	
6	Manager	☐	
7	Administrator	☐	
8	Other (Specify the discipline) **……..**	☐	

Q5. Please specify your experience in the organisation

1	Less than 5 years	☐	☐
2	5-10 years	☐	
3	11-15 years	☐	
4	16-20 years	☐	
5	21-25 years	☐	
6	Over 25 years	☐	

Section B: Saudi Arabia Culture

		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Q1	Tribe values and norm has influenced employees' behaviour towards information security in the hospital.	☐	☐	☐	☐	☐
Q2	Hospital working values and norms has influenced hospital information security.	☐	☐	☐	☐	☐
Q3	Attitudes towards women have influenced hospital information security.	☐	☐	☐	☐	☐
Q4	Saudi Arabia national culture has influenced hospital employee attitudes towards information security.	☐	☐	☐	☐	☐

Section C: SA Hospital Leadership style

		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Q1	National culture has influenced SA health services leadership style.	☐	☐	☐	☐	☐
Q2	Hospital leadership sharing power style in managing the hospital has influenced the information security.	☐	☐	☐	☐	☐
Q3	Hospital leadership sharing vision with employees toward information security has influenced the information security culture.	☐	☐	☐	☐	☐
Q4	Hospital leadership towards information security has influenced the information security.	☐	☐	☐	☐	☐
Q5	SA hospital leadership style has influenced hospital employee attitudes towards information security.	☐	☐	☐	☐	☐

Section D: Employees trust

		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Q1	Trust among the employees has influenced the information secure.	☐	☐	☐	☐	☐
Q2	Trust between the employees and the management has influenced the information security.	☐	☐	☐	☐	☐
Q3	Understanding between the employees has influenced the information security.	☐	☐	☐	☐	☐
Q4	Social interaction among the employees has influenced the information security.	☐	☐	☐	☐	☐
Q5	Employees trust among themselves has influenced hospital employee attitudes towards information security.	☐	☐	☐	☐	☐

Section E: Role of Technology

		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Q1	Hospital intranet has influenced the information security culture.	☐	☐	☐	☐	☐
Q2	Hospital communication system has influenced the information security.	☐	☐	☐	☐	☐
Q3	Electronic information system has influenced the information security.	☐	☐	☐	☐	☐
Q4	Use of technology in the hospital has influenced the information security.	☐	☐	☐	☐	☐
Q5	Use of technology in the hospital has influenced hospital employee attitudes towards information security.	☐	☐	☐	☐	☐
Q6	Hospital communication system has influenced the employees trust in information security.	☐	☐	☐	☐	☐

Section F: Role of Multicultural Interaction

		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Q1	Employees' different languages have influenced the information security.	☐	☐	☐	☐	☐
Q2	Diversity of national culture of the employees has influenced the information security.	☐	☐	☐	☐	☐
Q3	Diversity in working values and norms of the employees has influenced the information security.	☐	☐	☐	☐	☐
Q4	Multicultural interaction in the hospital has influenced hospital employee attitudes towards information security.	☐	☐	☐	☐	☐
Q5	Multicultural has influenced hospital employee trust towards information security.	☐	☐	☐	☐	☐

Section G: Employees Training and Motivation

		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Q1	Employees training in information security have influenced the information security.	☐	☐	☐	☐	☐
Q2	Employees' motivation has influenced the information security.	☐	☐	☐	☐	☐
Q3	Employees' job satisfaction has influenced the information security.	☐	☐	☐	☐	☐
Q4	Employees training and motivation has influenced hospital employee attitudes towards information security.	☐	☐	☐	☐	☐

Section H: Hospital culture

		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Q1	Employees' attitude has influenced the employees' behaviour towards information security.	☐	☐	☐	☐	☐
Q2	Hospital culture has influenced the employees' behaviour towards information security.	☐	☐	☐	☐	☐

Section I: Employees behaviour

		Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
Q1	Employees' behaviour towards information security has influenced developing and implementing information security policy.	☐	☐	☐	☐	☐
Q2	Employees' behaviour towards information security has influenced promoting information security culture.	☐	☐	☐	☐	☐

Section J: Please comment on the cultural information security at your hospital.

……

……

……

……

……

……

……

Many thanks for completing the questionnaire

Appendix D: Information Security culture model evaluation: Interview design

De Montfort University

Information Security Culture Model Evaluation

Interviews with Key SA Health Services Personnel

Culture dimensions of information systems security in Saudi Arabia National Health Services

S. Al-umaran

March 2013

INTERVIEWEE <u>RESPONDENT PERSONAL BACKGROUND</u>

Name of the Interviewee : ---------- ----------

Hospital's Name ----------

Position in the Hospital ----------

Email Address ----------

How long have you been working in this hospital? ----------

Could you please describe your current roles and responsibility in the hospital?

<u>Section A</u>: <u>information security policy</u>

Q1: How do you describe the role and impact of Saudi culture on employees' attitude and behaviour towards information security policy?

……
……
……
……..

Q2: How do you describe the role and impact of Saudi culture on implementing effective information security policy?

……
……
……
…….

Section B: SA Hospital Leadership style

Q1: How do you describe the role and impact of hospital leadership style on the hospital information security culture?

……

……

……

……

Q2: in your view, what is the hospital leadership role in developing and implementing information security culture?

……

……

……

…….

Section C: Employees trust

Q1: How do you describe the current trust between the employees and the management on information security culture-implementation and respect to information security policy and instruction?

……
……
……
……

Q2: How do you describe the current trust between the employees on information security culture-implementation and respect to information security policy and instruction?

……
……
……
…….

Section D: Role of Technology

Q2: What is the role of use of technology on information security at your hospital information security culture?

……
……
……
……..

Section D: Role of Technology

Q1: What is the role of use of technology on information security at your hospital information security culture?

……
……
……
……

Section E: Role of Multicultural Interaction

Q1: What is the role of multicultural of hospital on information security culture?

……
……
……
……

Section F: Employees Training and Motivation

Q1: On your opinion what is the role of employees training and motivation towards creating effective information security culture on the hospital?

……
……
……
……

Section F: Practicality, reliability of the model

Q1: How does information security model helps in improving information security culture at your hospital?

……

……

……

……..

Q2: How practical the cultural information security model to your hospital?

……

……

……

…….

Appendix E: Published Academic paper and Published Poster in International Conference

1. Culture Dimensions of Information Systems in Saudi Arabia National Health Services, *International Journal of Social, Education, Economics and Management Engineering* Vol:9 No:2, 2015

2. Academic Poster, ICCSE 2015: XIII International Conference on Computer Science and Engineering, Kuala Lumpur, Malaysia, February, 12-13, 2015.